ON AUTOMORPHISMS OF FINITE

SIMPLE GROUPS

by

GAUTAM N. PANDYA

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

UNIVERSITY OF ALBERTA

EDMONTON, ALBERTA

February 1968

UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "On Automorphisms of Finite Simple Groups", submitted by Gautam N. Pandya in partial fulfilment of the requirements for the degree of Doctor of Philosophy.

ABSTRACT

The present work deals with the existence of a complement for the inner automorphism group Inn (G) in the automorphism group Au (G) of a finite simple group G. If G were an alternating group Alt (n) on n elements, $n > 4$, then the conjugation by a transposition obviously gives a complement for Inn (Alt (n)) in Au (Alt (n)), provided $n \neq 6$. For Alt (6) we prove that Inn (Alt (6)) has no complement in Au (Alt (6)).

Some necessary conditions for the existence of the complement are achieved when the group G is a finite Chevalley group. Let K denote the underlying base field of the corresponding Lie algebra $\mathcal{L}$ for the Chevalley group G. Let $q = |K| = p^n$ denote the number of elements in the field where p is the characteristic of K. Then the existence of the complement follows trivially for the following cases.

(1) The groups of type G_2, F_4 and E_8 with (finite) arbitrary base field K.

(2) The groups of type B_ℓ, C_ℓ, D_ℓ and E_7 provided p is equal to 2.

(3) The groups of type E_6 with

$$p^n \equiv 0 \text{ or } -1 \pmod 3 .$$

(4) The groups of type A_ℓ with

$$\text{g.c.d.}\,(|K|-1,\ \ell+1) = 1 .$$

We have developed a sufficient condition for the existence of the

complement for the remaining cases of the Chevalley groups. This condition is satisfied in the following cases.

(1) The groups of type B_ℓ, C_ℓ, E_7 and D_ℓ (even ℓ) provided

$$p^n \equiv 3 (\mathrm{mod}\ 4)\ ,\ p \text{ an odd prime.}$$

(2) The groups of type E_6 provided

$$p \equiv 1 (\mathrm{mod}\ 3) \quad \text{but} \quad p^n \not\equiv 1\ (\mathrm{mod}\ 9)$$

(3) The groups of type A_ℓ provided:

Either

(i) g.c.d. $(\ell+1,\ q-1) = d$, d odd; and

(ii) $(q-1) = du$ with g.c.d. $(d,u) = 1$.

Or

$$\ell+1 \equiv q-1 \equiv 2\ (\mathrm{mod}\ 4)$$

Finally the sufficient condition is relaxed and a complement is obtained for the groups of the type B_ℓ, C_ℓ and E_7 provided

$$p \equiv 1\ (\mathrm{mod}\ 4) \quad \text{and}$$

$$|K| = p^{2m+1}\ .$$

The sufficient condition is modified for the (Chevalley groups of) Twisted type and a complement is obtained for E_6^1 and A_ℓ^1 .

In the case of the groups of Ree and Suzuki the complements are readily obtained.

ACKNOWLEDGEMENTS

I am pleased to express here my gratitude to my supervisor, Professor R. Bercov for his helpful suggestions concerning the problems of this thesis. His patient editing has saved me from several errors.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

§ (I) Origin of the Problem

B. H. Neumann developed the idea of "Twisted Wreath Product" which he applied in the construction of an extension P^* of a non-trivial abelian group F^* by a prescribed non-trivial abelian group B in such a way that the lower central series of P^* becomes stationary at F^* and that, furthermore, a system of generators of P^* maps modulo F^* on a prescribed system of (at least two) generators of B (See [10]). This construction was also applied to the proof of a theorem of Auslander and Lyndon (See [11]).

It is well known that a minimal normal subgroup N of a finite group G is a direct product of conjugates of a simple group H (p. 131, [6]). R. Bercov ([1]) has shown that if

(*) H is non-abelian and $\mathrm{Inn}\,(H)$ has a complement in $\mathrm{Au}\,(H)$

then N has a complement C in G, and that G is a twisted wreath product of H by C. Using this he characterises those finite groups all of whose composition factors H satisfy (*) as "Iterated Twisted Wreath" products of simple groups satisfying (*).

The present work is an attempt to investigate some finite simple groups with respect to the condition (*) mentioned above.

The groups under consideration are the alternating groups, the (finite) Chevalley groups and the groups of "Twisted type" ([16], [3]).

The Chevalley groups are simple except the groups $A_1(2)$, $A_1(3)$, $B_2(2)$, $G_2(2)$ which are isomorphic to, respectively the symmetric group S_3 the Alternating group A_4, S_6 and a group of order 12096 which has a simple group of index 2 (See [2], [3]).

The twisted type groups $A_\ell^1(q^2)$, $\ell \geq 2$ and $E_6^1(q^2)$ where $q^2 = |K|$, are simple except $A_2^1(2^2)$ which is a solvable group of order 72. ([2]).

§ (II) <u>Structure of Simple Lie Algebras</u>

The following results can be easily found in the Literature (c.f. [6]).

Throughout our work $\mathcal{L}$ will denote a finite dimensional simple Lie algebra over the complex field unless stated otherwise.

<u>Definition (1.1)</u>

A representation of $\mathcal{L}$ is a homomorphism of $\mathcal{L}$ into the Lie algebra of linear transformations of a finite dimensional vector space M over the complex field.

M, in such a case, is also called an $\mathcal{L}$-module over the complex field.

<u>Definition (1.2)</u>

Let R be a representation of $\mathcal{L}$. A mapping α of $\mathcal{L}$ into the field of complex numbers is called a weight of M if there is a non-zero vector $x \in M$ such that for each $a \in \mathcal{L}$,

$$x(a^R - \alpha(a))^m = 0$$

for a suitable integer m.

The vectors satisfying this condition together with the zero vector of M form a subspace M_α of M called the weight space corresponding to the weight α. If $\mathcal{L}$ is a nilpotent Lie algebra then M_α is, in fact, a sub-module. If $M = M_\alpha$ then we say that M is a weight module for $\mathcal{L}$ w.r.t. the weight α.

Definition (1.3)

A sub-algebra H of $\mathcal{L}$ is called a Cartan sub-algebra if H is a nilpotent algebra and H is its own normaliser.

Definition (1.4)

For $b \in \mathcal{L}$ we define a linear transformation $ad.b$ of $\mathcal{L}$ such that

$$ad.b\,(x) = [b,x]\ ,\ x \in \mathcal{L}$$

where $[b,x]$ denotes the Lie product of b and x.

For a subset S of $\mathcal{L}$ we write $ad.S$ for the set

$$ad.S = \{ad.s \ : \ s \in S\}\ .$$

Proposition (1.5)

Let H be a Cartan sub-algebra of $\mathcal{L}$. Then

$$\mathcal{L} = \mathcal{L}_0 + \mathcal{L}_\alpha + \mathcal{L}_\beta + \ldots + \mathcal{L}_\delta$$

where $\alpha, \beta, \ldots, \delta$ are weights on ad.H, regarded as a Lie algebra of linear transformations of $\mathcal{L}$ ($\mathcal{L}$ regarded as a vector space) and $\mathcal{L}_0 = H$ where 0 is the zero weight.

This decomposition is called the Cartan decomposition. The weights associated with ad.H are called the roots of H in $\mathcal{L}$.

Definition (1.6)

If "tr" denotes the usual trace of a matrix then the form

$$f(a,b) = \text{tr.}\,(\text{ad. } a) \cdot (\text{ad. } b)$$

for a, b in $\mathcal{L}$ is a symmetric bilinear invariant form called the Killing form.

Cartan's Criterian for Semisimplicity (1.7)

A finite dimensional Lie algebra $\mathcal{L}$ over the field of complex numbers (or over any field of characteristic zero) is semisimple if and only if the Killing form is non-degenerate.

Hence if $\mathcal{L}$ is a simple Lie algebra of finite dimension over the complex field the Killing form is always non-degenerate. The restriction of this form to the Cartan sub-algebra H is also non-degenerate. Hence this form can be "extended" to the conjugate space H^* (see [6]). Since weights (and hence roots) of H for $\mathcal{L}$ are linear transformations over H we can speak of $f(\rho,\sigma)$ where ρ and σ are weights of H for $\mathcal{L}$. In what follows we shall write (ρ,σ) for $f(\rho,\sigma)$. If α is a root then $(\alpha,\alpha) \neq 0$.

Now the roots of H over $\mathcal{L}$ span H^* over the complex field.

In fact we can select a basis for H^* consisting only of roots such that all the other roots are linear combinations of these basis elements with rational coefficients.

Select a particular basis of H^* consisting only of the roots and consider the Q-space H_o^* spanned by this basis over the rational numbers Q. The space H_o^* can now be given a lexicographic ordering (p. 119, [6]). This is a total ordering and hence we can now speak of positive and negative roots.

In what follows by a root we always mean a non-zero root.

<u>Definition (1.8)</u>

A positive root is called simple if it cannot be written as a sum of two positive roots.

<u>Proposition (1.9)</u>

Let $\pi = \{\alpha_1, \alpha_2, \ldots, \alpha_\ell\}$ be the set of all simple roots (w.r.t. to the given ordering). Then:

(1) If $\alpha, \beta \in \pi$ and $\alpha \neq \beta$ then $\alpha - \beta$ is not a root.

(2) If $\alpha, \beta \in \pi$, $\alpha \neq \beta$ then $(\alpha, \beta) \leq 0$.

(3) The set π is a basis for the space H_o^* and if r is any positive root then

$$r = \sum_{i=1}^{\ell} \lambda_i \cdot \alpha_i$$

where λ_i are non-negative integers.

(4) If r is a positive root and $r \notin \pi$ then there is an $\alpha_i \in \pi$ such that $(r-\alpha_i)$ is a positive root.

It should be noted that the sum of two roots need not be a root.

The following results can be found in ([6]).

(1.10)

If r is a root then $-r$ is a root.

(1.11)

Let w be a weight (or a root) of H and α be an arbitrary root. Then the weights (the roots) of the form

$$w + i\alpha \, , \quad i \text{ an integer}$$

form an arithmetic progression with first term $w - p\alpha$, the difference α, and the last term $w + q\alpha$, where p and q are positive integers such that

$$\frac{2(w,\alpha)}{(\alpha,\alpha)} = p-q \, .$$

(1.12)

If w is a weight (or a root) of H and α is a root then

$$w' = w - \frac{2(w,\alpha)}{(\alpha,\alpha)} \cdot \alpha \, ,$$

Is also a weight (a root).

Since the bilinear form (ρ,σ) is non-degenerate it turns out that the mapping

$$S_\alpha : \rho \to \rho - \frac{2(\rho,\alpha)}{(\alpha,\alpha)} \alpha$$

is a linear transformation in H_o^* (p. 119, [6]). This is called the reflection determined by α. It leaves fixed every vector in the hyperplane orthogonal to α, sends α into $-\alpha$, and belongs to the orthogonal group of the form (ρ,σ).

Let W be the group generated by the linear transformations S_α of H_o^*. W is called the Weyl group of $\mathcal{L}$ (relative to H). As we observed above, the weights of the particular representation (and hence the roots) form a set of vectors which remains invariant under W.

Let π be the set of simple roots. π is also called a fundamental system of roots and the elements of π are called fundamental roots.

Let

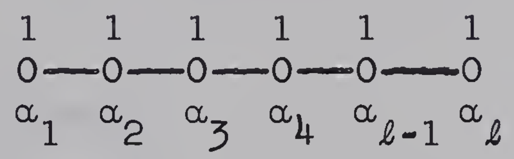
$$A_{ij} = \frac{2(\alpha_i,\alpha_j)}{(\alpha_i,\alpha_i)} \quad ; \quad i,j = 1,2,\ldots,\ell \ .$$

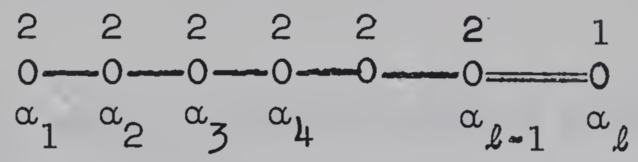
and let $A = (A_{ij})$ be the matrix with $(i,j)^{th}$ element A_{ij}. A is called the Cartan Matrix. Clearly every diagonal entry of this matrix is 2. As for the off-diagonal entries, either both A_{ij} and A_{ji} $(i \neq j)$ are zero or one is -1 and the other is -1, -2 or -3.

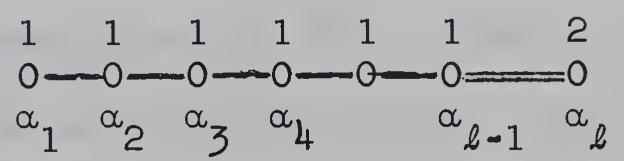
With each Cartan matrix A we associate The Dynkin Diagram. This consists of ℓ points in the plane, denoted by $\alpha_1, \alpha_2, \ldots, \alpha_\ell$, with α_i

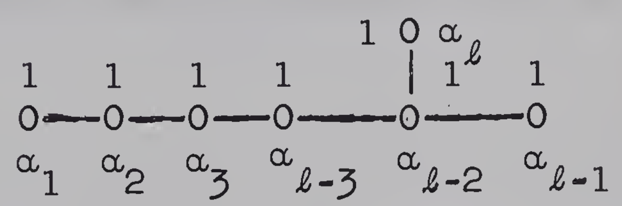
and α_j connected by $(A_{ij} \cdot A_{ji})$ lines. To each vertex α_i there is attached the "weight" (α_i,α_i). It turns out that for a simple Lie algebra $\mathcal{L}$ over the complex field the only possible Dynkin Diagrams are the following (p. 134, [6]):

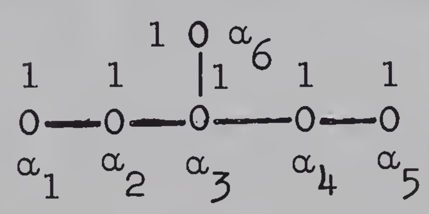
(1.13)

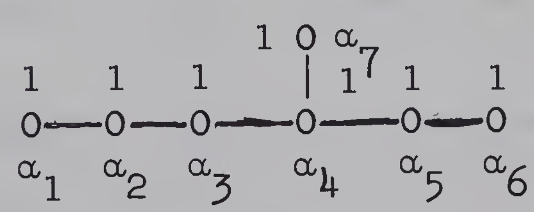
A_ℓ :  ; $\ell \geq 1$.

B_ℓ :  ; $\ell \geq 2$.

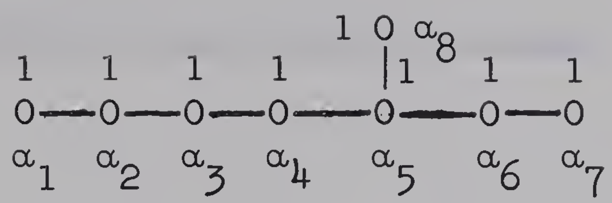
C_ℓ :  ; $\ell \geq 2$.

D_ℓ :  ; $\ell \geq 4$.

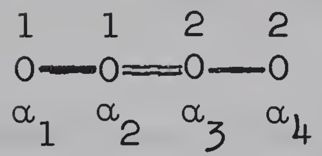
E_6 : 

E_7 : 

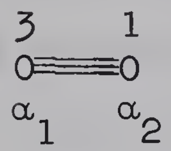
E_8 :



F_4 :



G_2 :



Let P_r denote the free abelian group generated by members of π, and P denote the group generated by the weights of H for $\mathcal{L}$ with respect to all the representations of $\mathcal{L}$. Then P_r is a subgroup of P . The following table gives information about P/P_r for different classes of simple Lie algebras over the complex field (p. 63, [3]).

(1.14)

A_ℓ : P/P_r is cyclic of order $(\ell+1)$.

B_ℓ, C_ℓ : P/P_r is of order two .

D_ℓ, odd ℓ : P/P_r is cyclic of order 4 .

D_ℓ, even ℓ : P/P_r is the Klein Four group.

E_6 : P/P_r is of order 3 .

E_7 : P/P_r is of order 2 .

G_2, F_4, E_8 : P/P_r = Identity .

§ (III) Chevalley basis and Chevalley groups

Let

$$\mathcal{L} = H + \mathcal{L}_\alpha + \mathcal{L}_\beta + \dots + \mathcal{L}_\delta$$

be a Cartan decomposition of the Simple Lie algebra over the complex field. Chevalley (§ I, [3]) showed that for each root r , an element e_r of (the one dimensional subspace) $\mathcal{L}_r$ and an element h_r (called a co-weight) of H can be chosen in such a way that if r and s are roots then:

(1) $[e_r, e_{-r}] = h_r$

(2) $[e_r, e_s] = \begin{cases} \pm (p+1)e_{r+s} & \text{if } r+s \text{ is a root} \\ 0 \text{ if } r+s & \text{is not a root.} \end{cases}$

(3) $[h_r \; e_s] = \frac{2(s,r)}{(r,r)} \; e_s$

(4) $[h_r \; h_s] = 0$.

where p is the largest integer such that $s-pr$ is a root.

The set $\{h_r : r \in \pi\}$ forms a basis for H . Hence the set

$$\{e_r : r \in R\} \cup \{h_r : r \in \pi\}$$

forms a basis for $\mathcal{L}$ such that the multiplication constants are all integers. Here R denotes the set of all roots (p. 208, [2]).

It can be seen that $ad.\, e_r$ is a nilpotent linear transformation. The same is true for $t(ad.\, e_r)$ where t is a

complex number. Hence $\exp(t(\mathrm{ad.}\ e_r))$ is an automorphism of $\mathcal{L}$ (p. 9, [6]). If $A_r(t)$ is the matrix representing the transformation $\exp(t(\mathrm{ad.}\ e_r))$ of $\mathcal{L}$ (in terms of the Chevalley basis) then the entries of $A_r(t)$ are polynomials in t with integer co-efficients.

Let K be an arbitrary (for our purpose finite) field. Let $\mathcal{L}_K$ be the set of all formal linear combinations of elements of the set

$$\{e_r : r \in R\} \cup \{h_r : r \in \pi\}$$

with elements of K as coefficients. Because of the Chevalley basis, $\mathcal{L}_K$ can be regarded as a Lie algebra over K.

If we replace the complex number t of $A_r(t)$ by an arbitrary element t' of the field K then (the matrix) $A_r(t')$ describes a linear transformation $x_r(t')$ of $\mathcal{L}_K$. $x_r(t')$, in fact, turns out to be an automorphism of $\mathcal{L}_K$.

Let $\mathcal{L}(K)$ be the group generated by the $x_r(t)$ for $r \in R$ and $t \in K$. $\mathcal{L}(K)$ is called the Chevalley group of type $\mathcal{L}$ over the field K. We will now denote $\mathcal{L}(K)$ by G, unless specified otherwise.

Let

$$U = \langle x_r(t) : t \in K,\ r > 0 \rangle$$

$$V = \langle x_r(t) : t \in K,\ r < 0 \rangle ,$$

where $\langle s \rangle$ is the subgroup generated by $s \subseteq G$.

Proposition (1.15)

If K is a finite field of characteristic p then U and V are p-Sylow subgroups of G.

U and V obviously generate G.

The following fundamental commutator relation was proved by Chevalley ([3]):

For any two positive roots r and s we have

(1.16)

$$x_r(t)x_s(u)x_r(t)^{-1} = x_s(u) \prod_{i\,j} x_{ir+js}(C_{ijrs}t^i u^j)$$

where the product is taken over all pairs (i,j) of positive integers such that $(ir+js)$ is a root, the pairs being arranged such that the roots $(ir+js)$ form an increasing sequence, and the C_{ijrs} are certain integral constants depending only on R (not on K).

Let r be a positive root and let

$$\chi_r = \{x_r(t) : t \in K\} \quad \text{and}$$

$$\chi_{-r} = \{x_{-r}(t) : t \in K\}$$

be the one-parameter subgroups of G. Here

$$x_r(t_1)x_r(t_2) = x_r(t_1 + t_2) \quad \text{and}$$

$$x_{-r}(t_1)x_{-r}(t_2) = x_{-r}(t_1 + t_2) .$$

Then there exists a homomorphism

$$\varphi_r : SL_2(K) \to < \chi_r, \chi_{-r} >$$

such that $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \to x_r(t)$ and $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \to x\text{-}r(t)$.

This homomorphism gives an easy method of carrying out computations in $< \chi_r, \chi_{-r} >$. If $\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(K)$ let

$$\omega_r = \varphi_r(\Omega) .$$

<u>Proposition (1.17)</u>

If $\{e_r : r \in \pi;\ h_r : r \in \pi\}$ is a Chevalley basis for $\mathcal{L}$ then for the automorphism ω_r of $\mathcal{L}$ we have

$$\omega_r(e_s) = \eta_s e_{w_r(s)}$$

where w_r is the reflection w.r.t. r and η_s is $\pm 1 \in K$.

We shall now introduce a certain abelian group of automorphisms of $\mathcal{L}_K$. Let $\hat{H}$ denote the group of characters of P_r ; i.e. the group of homomorphisms of P_r into the multiplicative group K^* of the field K . With the element χ of $\hat{H}$ we associate the linear transformation of $\mathcal{L}_K$ into itself which maps h_r into h_r and e_r into $\chi(r)e_r$ for each root r . This is, in fact, an automorphism of $\mathcal{L}_K$. We shall denote this automorphism by $h(\chi)$. The mapping which takes χ of $\hat{H}$ into the automorphism $h(\chi)$ of $\mathcal{L}_K$ is an isomorphism. Let $\hat{\mathcal{h}}$ denote the group of automorphisms of $\mathcal{L}_K$ generated by the $h(\chi)$. Since the character group $\hat{H}$ is abelian, $\hat{\mathcal{h}}$ is an abelian group.

Let H denote the group of those characters of P_r which can be extended to a character of P. Let $\mathfrak{h}$ denote the corresponding group of automorphisms of $\mathcal{L}_K$. With the help of the homomorphisms φ_r defined above, Chevalley has shown that $\mathfrak{h}$ is a subgroup of G.

Let $\hat{G}$ denote the group generated by G and $\hat{\mathfrak{h}}$. Then we have the following

<u>Proposition (1.18)</u>

G is a normal sub-group of $\hat{G}$ and $\hat{G}/_G \cong \hat{\mathfrak{h}}/\mathfrak{h}$. Also $G \cap \hat{\mathfrak{h}} = \mathfrak{h}$.

The values of $|\hat{\mathfrak{h}}/\mathfrak{h}|$ for different types of Chevalley groups are given by Chevalley (pp. 64, [3]) as follows:

(1.20)

Let $|K| = p^n = q$.

A_ℓ : $|\hat{\mathfrak{h}}/\mathfrak{h}| = \text{g.c.d.}(\ell+1, q-1)$

B_ℓ, C_ℓ, and E_7 : $|\hat{\mathfrak{h}}/\mathfrak{h}| = 1$ if q is even

$|\hat{\mathfrak{h}}/\mathfrak{h}| = 2$ if q is odd.

D_ℓ, odd ℓ : $|\hat{\mathfrak{h}}/\mathfrak{h}| = 1$ if q is even

$|\hat{\mathfrak{h}}/\mathfrak{h}| = 2$ if $q \equiv 3 \pmod 4$

$|\hat{\mathfrak{h}}/\mathfrak{h}| = 4$ if $q \equiv 1 \pmod 4$

D_ℓ, even ℓ : $|\hat{\mathfrak{h}}/\mathfrak{h}| = 1$ if q is even

$|\hat{\mathfrak{h}}/\mathfrak{h}| = 4$ if q is odd

E_6 : $|\hat{\mathfrak{h}}/\mathfrak{h}| = 1$ if $q \equiv 0$ or $-1 \pmod 3$

$|\hat{\mathfrak{h}}/\mathfrak{h}| = 3$ if $q \equiv 1 \pmod 3$.

G_2, F_4, E_8 : $|\hat{\mathfrak{h}}/\mathfrak{h}| = 1$.

Proposition (1.21)

Let $\overline{W}$ denote the group generated by $\hat{\mathfrak{h}}$ and the elements

$$\{\omega_r = \varphi_r(\Omega) : r \in \pi\} .$$

Then there is a homomorphism ζ of $\overline{W}$ onto the Weyl group W such that if $\omega \in \overline{W}$ and $\zeta(\omega) = w$ then $\omega\chi_r\omega^{-1} = \chi_{w(r)}$ and for $h(\chi) \in \hat{\mathfrak{h}}$, $\omega h(\chi)\omega^{-1} = h(\chi')$ where $\chi'(s) = \chi(w^{-1}(s))$ for all $s \in P_r$. Also the kernel of ζ is $\hat{\mathfrak{h}}$.

Proposition (1.22)

(1) The normalizer of U (of V) in $\hat{G}$ is $U\hat{\mathfrak{h}}$ ($V\hat{\mathfrak{h}}$) .

(2) The normalizer of U (of V) in G is $U\mathfrak{h}$ ($V\mathfrak{h}$) .

Let $\omega(w) \in \overline{W}$ such that $\zeta(\omega(w)) = w \in W$. Select $\omega(w) \in \overline{W}$ for each $w \in W$. Then these $\omega(w)$ form a set of coset representatives for $\hat{\mathfrak{h}}$ in $\overline{W}$.

For $w \in W$ let U_w denote the group generated by those χ_r for which $r > 0$ and $w(r) < 0$. Chevalley proved the following decomposition (Bruhat decomposition) for G. (for $\hat{G}$). (thm. 2, p. 42, [3]).

Proposition (1.23)

$\hat{G}(G)$ is the disjoint union of the double cosets $U\hat{\mathfrak{h}}.\ \omega(w) \cdot U_w$ $(U\mathfrak{h} \cdot \omega(w)U_w)$. An element x of $\hat{G}$ (of G) can be uniquely expressed as

$$x = u_1 \cdot h(\chi) \cdot \omega(w) \cdot u_2$$

where $u_1 \in U$, $u_2 \in U_w$, $w \in W$ and $h(\chi) \in \hat{\mathfrak{h}}$ $(h(\chi) \in \mathfrak{h})$.

§ (IV) Automorphisms of Chevalley groups

First observe that all Chevalley groups G are centreless. (In fact all except $A_1(2)$, $A_1(3)$, $B_2(2)$ and $G_2(2)$ are simple). (p. 63, [3]). Hence the group G and its inner automorphism group I are isomorphic.

Conjugation by elements $h(\chi)$ of $\hat{\mathfrak{h}}$ yields automorphisms of I and hence of G as I is always normal in $Au(G)$. Since elements of $\hat{\mathfrak{h}}$ as automorphisms of $\mathcal{L}_K$ are described by diagonal matrices, these automorphisms are called diagonal automorphisms. The automorphism of G corresponding to $\chi \in \hat{H}$ will be denoted by $d(\chi)$.

For $x_r(t) \in G$ and $\chi \in \hat{H}$ we have

(1.24)

$$x_r(t)^{d(\chi)} = x_r(\chi(r) \cdot t) .$$

The group of diagonal automorphisms is denoted by $\hat{D}$, and $< d(\chi) \mid \chi \in H >$ by D.

Now the automorphisms of K with $|K| = p^n$ form a cyclic group of order n generated by the automorphism $\bar{p} : K \to K$ given by

$$\bar{p}(t) = t^p \quad .$$

The automorphism $f : G \to G$ induced by

(1.25)

$$x_r(t)^f = x_r(t^p) \quad .$$

is called (for obvious reason) a field automorphism of G. The group F generated by f is a cyclic group of order n.

Finally another type of automorphism of G is obtained from the symmetries of the corresponding Dynkin diagram. By a symmetry of the Dynkin diagram we mean a permutation σ of its vertices which preserves connectedness; i.e. such that if α_i and α_j are connected by i lines, then so are $\sigma(\alpha_i)$ and $\sigma(\alpha_j)$.

The only possible symmetry for the diagram of type B_ℓ, C_ℓ, A_1, G_2, F_4 and E_7 and E_8 is the identity permutation.

The following are the non-trivial symmetries in the remaining cases (pp. 280-81, [6]):

(1.26)

$$A_\ell,\ \ell \geq 2 : \ \alpha_i \to \alpha_{\ell+1-i} \quad . \quad i = 1,2,3,\ldots,\ell \ .$$

D_ℓ, $\ell \geq 5$: $\alpha_i \to \alpha_i$ $\quad i \leq \ell-2$

$\alpha_{\ell-1} \to \alpha_\ell$

$\alpha_\ell \to \alpha_{\ell-1}$

D_4 : Each permutation of α_i, α_3 and α_4 gives a symmetry. The group of symmetries, therefore, is isomorphic to the symmetric group S_3 on three elements.

E_6 : $\alpha_6 \to \alpha_6$

$\alpha_i \to \alpha_{6-i}$; $\quad i \leq 5$.

The symmetry σ for the Dynkin diagram gives rise to an automorphism of the Chevalley group induced by

(1.27)

$$x_r(t)^\sigma = x_{\sigma(r)}(t) .$$

We may obtain additional automorphisms for groups of type B_2, G_2 and F_4 if the base field K is a perfect field of characteristic 2 and 3. If the group is of type G_2 there is an automorphism such that

$$x_\alpha(t)^\sigma = x_\beta(t)$$

and

$$x_\beta(t)^\sigma = x_\alpha(t^3)$$

where α and β are fundamental roots such that $2\alpha + 3\beta$ is also a root.

For the groups of type B_2 we proceed as follows:
Let α and β be fundamental roots such that $2\alpha + \beta$ is a root.
If r is a root define $\bar{r}$ as

$$\bar{r} = \frac{\Psi(r)}{\delta(r)}$$

where

$$\Psi(\alpha) = \beta \ , \qquad \Psi(\beta) = 2\alpha$$

and $\delta(r) = 1$ or 2 depending on whether r is a short or a long root.
The mapping

$$x_r(t) \to x_{\bar{r}}(t^{\delta(\bar{r})})$$

induces an automorphism of the group.

If the group is of type F_4 with Dynkin diagram

$$\begin{array}{ccccccc} 1 & & 1 & & 2 & & 2 \\ 0 & - & 0 & = & 0 & - & 0 \\ c & & a & & b & & d \end{array} \quad .$$

Let Ψ be the mapping:

$$\Psi(a) = b \ , \quad \Psi(b) = 2a \ , \quad \Psi(c) = d \ , \quad \Psi(d) = 2c \ .$$

For each root r, let

$$\bar{r} = \frac{\Psi(r)}{\delta(r)} \ ,$$ where $\delta(r)$ is as before. Then

$$x_r(t) \to x_{\bar{r}}(t^{\delta(\bar{r})})$$

induces an automorphism of the group.

All these are called graph automorphisms of G. We shall denote by Γ the group generated by the graph automorphism.

Steinberg has proved the following elegant structure theorem for the automorphism group $Au(G)$ of G (3.2, [14]).

Proposition (1.28)

An automorphism σ of a finite Chevalley group G can be expressed as

(1.24)

$$\sigma = g.f.d.i$$

where $g \in \Gamma$, $f \in F$, $d \in D$ and $i \in I$. Also g and f are uniquely determined by σ.

§ (V) Groups of Twisted Type (R. Steinberg)

After the discovery of the Chevalley groups, Ree ([11]) identified the groups of type A_ℓ, B_ℓ, C_ℓ, D_ℓ, with certain of the classical groups. He also identified the groups $G_2(K)$ with the groups of type G_2 discovered by Dickson in 1901 and 1905 ([4], [5]). But the Unitary groups and the second class of orthogonal groups in even diemension do not arise as a Chevalley group. It is therefore natural to suppose that a modification of the method of Chevalley might yield some new class of simple groups. Such a construction was developed by R. Steinberg ([16]), and indeed led to the discovery of a new family of simple groups. We shall adopt the approach used by Steinberg ([16]).

Let $G = \mathcal{L}(K)$ be any Chevalley group which admits a (non-trivial)

graph automorphism taking $x_r(t)$ to $x_{\bar{r}}(t)$ where $r \to \bar{r}$ is a symmetry of the Dynkin diagram. We suppose that G admits a field automorphism $x_r(t) \to x_r(\bar{t})$ of the same order. Now consider the automorphism

$$x_r(t) \xrightarrow{\sigma} x_{\bar{r}}(\bar{t})$$

of G obtained by combining these two automorphisms. Let U^1 and V^1 be the set of elements of U and V respectively which are invariant under σ. Finally let $G^1 = \mathcal{L}^1(K)$ be the group generated by U^1 and V^1. Then the groups G^1 turn out to be simple except for $A_2^1(2^2)$ which is a solvable group of order 72.

The Chevalley groups of type A_ℓ, D_ℓ and E_6 have non-trivial graph automorphism of order two. If the base field K has $q = p^{2n}$ elements then G possesses a field automorphism of order 2. The construction of Steinberg gives us the twisted type $A_2^1(K)$, $\ell \geq 2$, $D_\ell^2(K)$, $\ell \geq 4$; and $D_6^1(K)$.

The groups $D_4(K)$ have a graph automorphism of order three. Hence we get $D_4^2(K)$ when K has p^{3n} elements.

The groups $E_6^1(p^{2n})$ and $D_4^2(p^{3n})$ were simple finite groups hitherto unknown.

An element $h(\chi)$ of $\mathfrak{h}$ can be shown to be in G^1 if and only if χ is a self conjugate character of P_r which can be extended to a self conjugate character of P; i. e.

$$\chi(\bar{r}) = \overline{\chi(r)} \quad \text{for} \quad r \in P .$$

The automorphism of the twisted type group G^1 were also determined by Steinberg ([14]).

Let $\hat{h}^i$ be the group of $h(\chi) \in \hat{h}$ where χ is a self conjugate character of P_r ; and let $\hat{G}^1$ be the group generated by G^1 and $\hat{h}^1$. Then G^1 is normal in G^1 ; $G^1 \cap \hat{h}^1 = h^1$ and $\hat{G}^1 / G^1 \cong \hat{h}^1 / h^1$. Conjugation by elements of $\hat{G}^1$ yields automorphisms of G^1 . These automorphisms induced by $\hat{h}^1$ are called diagonal automorphism G^1 .

We have (see e.g. p. 233, [2])

(1.30)

$$[\hat{G}^1 : G^1] = [\hat{h}^1 : h^1] = d$$

where

$$\begin{aligned} d &= (\ell+1,\ q+1) \quad \text{for} \quad A_\ell^1(q) \ , \\ &= (4,\ q^\ell+1) \quad \text{for} \quad D_\ell^1(q) \\ &= (3,\ q+1) \quad \text{for} \quad E_6^1(q) \end{aligned}$$

and $$d = 1 \quad \text{for} \quad D_4^2(q) \ .$$

Automorphisms of K determine automorphisms of G^1 (just as for the non-twisted groups).

Steinberg has shown that any automorphism σ of a group of twisted type G^1 can be expressed in the form f.d. i where f, d, i are respectively, field, diagonal, and inner automorphisms of G^1 . As before, f is uniquely determined by σ .

CHAPTER 2

AUTOMORPHISMS OF Alt (n) , $n \geq 5$.

§ (I) Preliminary Observations

The alternating groups Alt (n) are non-abelian simple groups for $n \geq 5$.

It is well-known (see p. 314, [12]) that

$$\mathrm{Au}(S(n)) \cong \mathrm{Au}(\mathrm{Alt}\ (n)) \ ; \qquad n \geq 5$$

and

$$\mathrm{Au}(S(n)) \cong S(n) \ ; \qquad n > 6 \quad \text{and} \quad n = 5 \ .$$

Hence except for Alt (6), the automorphisms of Alt (n) , $n \geq 5$, are precisely those which are obtained by conjugation by elements of $S(n)$.

Since any transposition is an odd permutation and has order two, it obviously generates a complement for Inn (Alt (n)) in Au(Alt (n)) . Hence:

Lemma 2.1

For $n \neq 6$, $n \geq 5$, Inn (Alt (n)) has a complement in Au(Alt (n)) .

§ (II) Au(Alt (6))

In this case (see p. 314, [13])

$$[\ Au(S(6)) : Inn\ (S(6))\ ] = 2$$

and

$$Au(S(6)) \cong Au(Alt\ (6))$$

hence there is an outer automorphism of Alt (6) which is not obtained by taking conjugations by elements of S(6) . Miller (see [9]) has given an explicit construction of such an outer automorphism. Since this outer automorphism is of order two,

$$\frac{Au(Alt\ (6))}{Inn(Alt\ (6))}$$

is easily seen to be the Klein Four group.

For Au(Alt (6)) we shall prove the following theorem:

Theorem (2.2)

Inn (Alt (6)) has no complement in Au(Alt (6)) .

Proof.

Suppose the contrary and let C be a complement for Inn(Alt (6)) in Au(Alt (6)) . Then C must be a Four group.

If $x \in S(6)$ let x^* denote the automorphism of Alt (6) obtained by taking conjugation of Alt (6) by x.

Since $Au(S(6)) \cong Au(Alt\ (6))$ we shall not distinguish between automorphisms of Alt (6) and of $S(6)$. Since C is a Four group, C must contain two outer automorphisms α and β of $S(6)$ and one inner automorphism x^*, $x \in S(6)$. We have

$$x^{*2} = \alpha^2 = 1 , \quad \alpha x^* = x^* \alpha = \beta ,$$

and $x \notin$ Alt (6). Hence x is a transposition or a product of three transpositions.

For $y \in A_6$ since

$$\alpha x^* = x^* \alpha$$

we have

$$\alpha x^*(y) = x^* \alpha(y)$$

$$\therefore \ \alpha(x^{-1} y x) = x^*(\alpha(y)) = x^{-1} \alpha(y)\, x$$

$$\therefore \ \alpha(x)^{-1} \alpha(y)\, \alpha(x) = x^{-1} \alpha(y)\, x \qquad \text{i.e.}$$

$x(\alpha(x))^{-1}$ centralizes each element of A_6. But the centralizer of A_6 in S_6 is the identity. Hence

$$x(\alpha(x))^{-1} = 1 . \quad \text{i.e.}$$

$$\alpha(x) = x , \quad \text{i.e.}$$

α fixes x; where x is a transposition or a product of three distinct transpositions.

Now each automorphism of $S(6)$ (and hence of A_6) is of the form $y^*\alpha$ where y^* is an inner automorphism of $S(6)$. Hence each automorphism $(y^*\alpha)$ of S_6 transforms x into a conjugate, since α fixes x. But Miller has shown that there is an outer automorphism θ which transforms each transposition into a product of three distinct transpositions and vice versa. This means θ does not take x into a conjugate of x. This contradiction proves the theorem.

CHAPTER 3

PRELIMINARIES FOR (FINITE)CHEVALLEY GROUPS

§ (I) Preliminary results and observations.

Let $\pi = \{\alpha_1, \alpha_2, \ldots, \alpha_\ell\}$ be a fundamental system of roots. Then π constitutes a basis for the space H_o^* and H_o^* contains all the weights.

It is shown by Harish-Chandra (see [8]) that there is a family of so called fundamental weights $\{p_1, p_2, \ldots, p_\ell\}$ of representations of the Lie algebra such that

$$p_i(h_{\alpha_j}) = \delta_{ij} \tag{3.1}$$

where h_{α_j} is the co-weight corresponding to the fundamental root α_j and δ_{ij} is the Kronecker delta. He also showed that this family forms a basis for the group P of weights.

Since $p_i \in H_o^*$ we have

$$p_i = \sum_j \lambda_{ij} \alpha_j \tag{3.2}$$

Hence

$$p_i(h_{\alpha_j}) = \sum_k \lambda_{ik}\alpha_k(h_{\alpha_j})$$

$$= \sum_k \lambda_{ik} \frac{2(\alpha_j, \alpha_k)}{(\alpha_j, \alpha_k)}$$

$$= \sum_k \lambda_{ik} \cdot A_{jk}$$

where (A_{ij}) is the Cartan matrix.

If $A' = (A'_{ij})$ denotes the transpose of $(A_{ij}) = A$ then

$$p_i(h_{\alpha_j}) = \sum_k \lambda_{ik} \cdot A'_{kj} .$$

where $$p_i(h_{\alpha_j}) = \delta_{ij} .$$

Hence

(3.3) $$\sum_k \lambda_{ik} \cdot A'_{kj} = \delta_{ij} .$$

If $\Lambda = (\lambda_{ij})$ denotes the matrix whose (ij) th entry is λ_{ij} then (3.3) shows that

(3.4) $$\Lambda A' = I$$

where I is the identity matrix.

Hence

(3.5) $$\alpha_j = \sum_{i=1}^{\ell} A_{ij} \cdot p_i ; \qquad A = (A_{ij}) .$$

This relation between fundamental roots and fundamental weights will be used in constructing certain diagonal automorphisms of the Chevally group.

§ (II) Some easy cases.

We first dispose of some easy cases:

Lemma (3.6)

If Γ is the graph automorphism group and F is the field automorphism group of the Chevalley group G then $\Gamma F = F\Gamma$ is a group and ΓF is a complement for $\mathrm{Inn}(G)$ in $\mathrm{Au}(G)$ in the following cases:

(1) G is of type G_2, F_4 or E_8 over an arbitrary field K.

(2) G is of type B_ℓ, C_ℓ, E_7, D_ℓ, provided the characteristic of k is 2.

(3) G is of type E_6 with $|k| \equiv -1$ or $0 \pmod 3$

(4) G is of type A_ℓ with g.c.d. $(\ell+1, |K| -1) = 1$.

Proof

Let g be a graph automorphism and let f be a field automorphism of G. Then it can easily be seen that

$$U^{gfg^{-1}} = U \quad \text{and}$$

$$V^{gfg^{-1}} = V .$$

Also, if α is a fundamental root and $1 \in K$, 1 being the identity,

then

$$x_{\alpha}(1)^{gfg^{-1}} = x_{\bar{\alpha}}(1)^{fg^{-1}} = x_{\bar{\alpha}}(1)^{g^{-1}} = x_{\alpha}(1) .$$

Hence (cf. 5.7, [16]) gfg^{-1} is a field automorphism. In fact, if g is arising from a symmetry of the Dynkin diagram then $gfg^{-1} = f$. Hence $\Gamma F = F\Gamma$ is a group.

We now show that

$\mathrm{Inn}\,(G) \cap \Gamma F$, then

$x = g.f$, $g \in \Gamma$, $f \in F$.

$1 = g.f.x^{-1}$; $x \in \mathrm{Inn}\,(G)$.

Hence this is a presentation of the identity automorphism 1 in terms of a graph automorphism g, a field automorphism f , and an inner automorphism x . Since g and f are uniquely determined by 1 (see [14]) it follows that

$$f = g = 1 .$$

Hence

$$x = gf = 1 , \quad \text{and}$$

$$\mathrm{Inn}\,(G) \cap \Gamma F = 1 .$$

Now observe that for (cf. Ch.I,(1.20)) the groups G of this lemma, we have

$$\hat{H} = H ; \quad \text{hence}$$

$$\hat{D} = D \text{ and } \hat{D} \subseteq \mathrm{Inn}\,(G) .$$

Thus all diagonal automorphisms are inner automorphisms and $\mathrm{Inn}\,(G)$ and ΓF generate $\mathrm{Au}\,(G)$.

This proves the lemma.

CHAPTER 4

SOME NECESSARY CONDITIONS FOR CHEVALLEY GROUPS

Let G be a finite Chevalley group and suppose $\mathrm{Inn}\,(G)$ has a complement C in $Au(G)$. Then

$$\mathrm{Inn}\,(G) \cap C = 1 \; ; \quad \mathrm{Inn}\,(G) \cdot C = Au(G) \; .$$

Since $\mathrm{Inn}\,(G)$ is normal in $Au(G)$, $\mathrm{Inn}\,(G) \cdot \hat{D} = \hat{D} \cdot \mathrm{Inn}\,(G)$ is a group where $\hat{D}$ is the group of diagonal automorphism of G.

Now according to Steinberg (see [14])

$$Au(G) = \Gamma F \hat{D} \cdot I$$

where $I = \mathrm{Inn}\,(G)$. Hence

$$\frac{Au(G)}{I} = \frac{\Gamma I}{I} \cdot \frac{FI}{I} \cdot \frac{\hat{D} \cdot I}{I} \quad .$$

As C is a complement for I in $Au(G)$,

(4.1) $$C \cong \frac{\Gamma I}{I} \cdot \frac{FI}{I} \cdot \frac{\hat{D} \cdot I}{I} \quad .$$

Let

$$C_1 = C \cap \hat{D}I$$

$$C_2 = C \cap FI$$

and

$$C_3 = C \cap \Gamma I \; .$$

Since

$$Au(G) = C \cdot I$$

We have $\quad f = c_2 \cdot i_2 , \quad c_2 \in C_2 , \quad i_2 \in I$

where $F = < f >$; $f^n = 1 \quad (|K| = p^n)$

and

$$g = c_3 \cdot i_3 ; \quad c_3 \in C_3 , \quad i_3 \in I ,$$

for any $g \in \Gamma$.

Since the Γ-part and F-part of an element σ of $Au(G)$ where

$$\sigma = g.f.d.i.$$

are uniquely determined by σ it follows that

$$\Gamma \cap I = F \cap I = 1 .$$

Hence $f = c_2 \cdot i_2$ and $f^n = 1$ gives

$$c_2^n = 1 \text{ and}$$

(4.2) $$C_2 = <c_2> ; \quad c_2^n = 1 .$$

$$\text{i.e. } C_2 \cong F .$$

It can be easily seen that

(4.3) $$C_3 \cong \Gamma .$$

Hence C_3 is of order two except for the group of type $D_4(K)$ where it is isomorphic to the symmetric group $S(3)$ on three elements.

The group $\widehat{DI}/I \cong \widehat{G}/G \cong \widehat{h}/h$ is a cyclic group except for G of type $D_\ell(K)$ with even ℓ, where it is a Four group. If $id(\chi)$ is a generator of $\widehat{DI}/I$ let

$$d(\chi) = c_i \cdot i_1 \ ; \quad c_1 \in C_1 \ , \ i_1 \in I$$

then it can be seen that

$$C_1 = < c_1 > \ ; \quad c_1^u = 1$$

where $u = |\widehat{H}/H|$

except for $D_{2\ell}(K)$ when C_1 is a Four group.

Since $\widehat{DI}$ is a normal subgroup of $Au(G)$ (see p. 608, [14]) it follows that C_1 is a normal subgroup of C.

Also

$$\Gamma F \cap \widehat{DI} = F \cap \Gamma = 1$$

leads us to

$$C_3 \ C_2 \ \cap C_1 = C_2 \cap C_3 = 1 \ .$$

We saw before that $gfg^{-1} \in F$ for $f \in F$, $g \in \Gamma$.

Let $gfg^{-1} = \bar{f}$. Let $g = c_3 \, i_3$, $f = c_2 \, i_2$ and $f = \bar{c} \, \bar{i}$.

$$\therefore \quad (c_3 \, i_3)(c_2 \, i_2)(c_3 \, i_3)^{-1} = \bar{c} \, \bar{i} \ .$$

$(c_3 \, c_2 \, c_3)i = \bar{c} \, \bar{i}$. But $C \cap I = 1$. Hence

$c_3 \, c_2 \, c_3 = \bar{c}$, $i = \bar{i}$. This shows that C_3 normalizes C_2 and hence, $C_3 \, C_2 = C_2 \, C_3$ is a group.

Finally (4.1) leads us to $C = C_3 \, C_2 \, C_1$.

Hence we have proved the following :

Theorem 4.5

If C is a complement for I in $Au(G)$ then

(1) $C = C_3 \cdot C_2 \cdot C_1$ where

$C_1 = C \cap DI$

$C_2 = C \cap FI$

$C_3 = C \cap \Gamma I$.

(2) C_1 is a normal subgroup of C and $C_2 \, C_3 = C_3 \, C_2$ is a group.

(3) $C_3 \cap C_2 = C_3 \, C_2 \cap C_1 = 1$.

Corollary 4.6

If G is a group of type B_ℓ, C_ℓ, or E_7 then under the hypothesis of Theorem (4.5)

$$C = C_3 \times C_2 \times C_1 ,$$

unless G is of type B_2 and K is perfect of characteristic 2 in which case we have $C = C_3 \, C_2 \times C_1$.

Proof

Elements of C_2 and C_3 normalizes C_1. But for the groups under consideration

$$[\frac{\widehat{DI}}{I}] \cong \widehat{G}/G \cong \widehat{h}/h$$

where $|\widehat{H}/H| = 2$. Hence $|C_1| = 2$. This means elements of C_2 and C_3 centralize elements of C_1. The conclusion follows from the remaining results of Theorem 4.5, and the fact that $c_3\, c_2 = c_2\, c_3$, unless G is of type B_2 and K is perfect of characteristic 2.

CHAPTER 5

A SUFFICIENT CONDITION FOR CHEVALLEY GROUPS

We shall now give a sufficient condition for the existence of a complement for I in $Au(G)$ where G is a finite Chevalley group.

If $\chi \in H$, i.e. χ is a homomorphism of P_r into K^*, and φ is a symmetry for the Dynkin diagram, then the composition $\chi \circ \varphi$ is a homomorphism of P_r into K^* since φ permutes the basis $\{\alpha_1, \alpha_2, \ldots, \alpha_\ell\}$.

With this observation we are now ready to prove

Theorem (5.1)

Suppose D has a non-trivial complement C' in $\hat{D}$ such that

(5.2) For each $d(\chi) \in C'$, $d(\chi \circ \varphi) \in C'$ for every symmetry φ of the Dynkin diagram. Then

$$C = \Gamma F C'$$

is a complement for I in $Au(G)$.

Proof

Let f be the field automorphism of G such that, for $x_r(t) \in G$,

$$x_r(t)^f = x_r(t^p) .$$

We know that f generates F .

Let $d(\chi) \in C'$ and let α be a fundamental root. Then

$$x_\alpha(t)^{fd(\chi).f^{-1}} = x_\alpha(t^p)^{d(\chi).f^{-1}}$$

$$= x_\alpha(\chi(\alpha).t^p)^{f^{-1}}$$

$$= x_\alpha(\chi(\alpha)^{p^{n-1}} . t)$$

$$= x_\alpha(\chi^{p^{n-1}}(\alpha).t)$$

$$= x_\alpha(t)^{d(\chi^{p^{n-1}})}$$

$$= x_\alpha(t)^{d(\chi)^{p^{n-1}}}$$

Similarly

$$x_{-\alpha}(t)^{f.d(\chi)f^{-1}} = x_{-\alpha}(t)^{d(\chi)^{p^{n-1}}} .$$

Since G is generated by the χ_{α_i} and $\chi_{-\alpha_i}$ it follows that

$$fd(\chi).f^{-1} = d(\chi)^{p^{n-1}}$$

and f normalizes C' . Hence F normalizes C' . Since $|\hat{D}/D| > 1$, graph automorphisms arises only from symmetries.

Let g be a graph automorphism of G , and let φ be the corresponding symmetry of the Dynkin diagram. For a fundamental root α , and for $d(\chi) \in C'$

$$\begin{aligned} x_\alpha(t)^{g.d(\chi)g^{-1}} &= x_{\varphi(\alpha)}(t)^{d(\chi)g^{-1}} \\ &= x_{\varphi(\alpha)}(\chi(\varphi(\alpha)).t)^{g^{-1}} \\ &= x_{\varphi^{-1}.\varphi(\alpha)}(\chi \circ \varphi(\alpha).t) \\ &= x_\alpha(\chi \circ \varphi(\alpha).t) \\ &= x_\alpha(t)^{d\,(\chi \circ \varphi)} \end{aligned}$$

Similarly

$$x_{-\alpha}(t)^{g.d(\chi).g^{-1}} = x_{-\alpha}(t)^{d(\chi \circ \varphi)} .$$

Hence

$$gd(\chi)g^{-1} = d(\chi \circ \varphi) .$$

By our hypothesis (5.2) Γ normalizes C' . Hence $C = \Gamma F C'$ is a group.

Let $\sigma \in C \cap I$.

Then $\sigma = g.f.d(\chi) = i$ for some $g \in \Gamma$, $f \in F$, $d(\chi) \in C'$, $i \in I$.

$\therefore$ $gfd(\chi)\, i^{-1} = 1$ and by (3.2 , [14])

$g = f = 1$

$\therefore$ $d(\chi) = i$, $d(\chi) \in C'$, $i \in I$.

Since C' is a complement for D in $\hat{D}$ and $\hat{D} \cap I = D$ we have $d(\chi) = i = 1$.

$$\therefore \quad C \cap I = 1 .$$

Since C contains Γ and F and CI contains $C'D = \hat{D}$ it follows that $CI = Au(G)$.

This proves the theorem.

CHAPTER 6

THE CHEVALLEY GROUPS

We shall now try to verify the sufficient condition for different types of Chevalley groups.

§ (I) The Groups of Type B_ℓ, $\ell \geq 2$.

The Cartan Matrix is

$$A = (A_{ij}) = \begin{bmatrix} 2 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & \cdots & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & -2 & 2 \end{bmatrix}$$

Now in this case

$$(6.1) \qquad \widehat{D}/D \cong \widehat{\mathfrak{h}}/\mathfrak{h} \cong \widehat{H}/H \; ; \; |\widehat{\mathfrak{h}}/\mathfrak{h}| = 2 = |\widehat{H}/H| = |P/P_r|$$

if $|K|$ is odd.

If $\{p_1, p_2, \ldots, p_\ell\}$ are fundamental weights then by (3.5)

$$\alpha_j = \sum_{i=1}^{\ell} A_{ij} \cdot p_i \quad .$$

Hence

(6.2)
$$\alpha_1 = 2p_1 - p_2$$

$$\alpha_2 = -p_1 + 2p_2 - p_3$$

$$\alpha_3 = -p_2 + 2p_3 - p_4$$

$$. \quad . \quad . \quad .$$

$$\alpha_{\ell-2} = -p_{\ell-3} + 2p_{\ell-2} - p_{\ell-1}$$

$$\alpha_{\ell-1} = -p_{\ell-2} + 2p_{\ell-1} - 2p_\ell$$

$$\alpha_\ell = -p_{\ell-1} + 2p_\ell \, .$$

Since $|P/P_r| = 2$ and $\alpha_i \in P_r$ it follows that $2p_i \in P_r$ for $i = 1, 2, 3, \ldots, \ell$. Hence

$$p_1, p_2, p_3, \ldots, p_{\ell-3}, p_{\ell-2}, p_{\ell-1} \in P_r$$

$$p_\ell \notin P_r \text{ and } 2p_\ell \in P_r \quad .$$

Since the Dynkin diagram of B_ℓ has no non-trivial symmetries for odd p the Chevalley groups of type B_ℓ $(\ell \geq 2)$ have no non-trivial graph automorphisms. Hence a complement for D in $\widehat{D}$ is sufficient to give a complement for $\mathrm{Inn}(G)$ in $\mathrm{Au}(G)$ (Theorem 5.1).

We now prove the following:

Lemma 6.3

If $| K | \equiv 3 \pmod 4$ then a complement C' for D in $\hat{D}$ exists.

Proof.

In fact we shall construct C'.

The elements of $\hat{D}$ are of type $d(\chi)$ where χ is a character of P_r.

Let us define a mapping χ of P_r into the multiplicative group K^* of K, such that

$$\chi(\alpha_1) = -1 \; ; \quad \chi(\alpha_i) = 1 \quad \text{for} \quad i = 1 .$$

Since the fundamental system $\{\alpha_1, \alpha_2, \alpha_3, \ldots , \alpha_\ell\}$ forms a basis for the group P_r, χ can be extended to a homomorphism of P_r. We shall denote this homomorphism also by χ.

Our next objective is to show that this homomorphism χ cannot be extended to a character of P. Then since

$$C' = < d(\chi) >$$

is of order two, it is a complement for D in $\hat{D}$.

Let a denote the generator of K^*. Then

$$-1 = a^{(q-1)/2} \quad , \quad q = |K| \quad .$$

As $q \equiv 3 \pmod 4$, $(\frac{q-1}{2})$ is an odd number. Since the order of a is the even number $q-1$, an odd power of a cannot be equal to an even power of a.

Suppose χ can be extended to a character of P, and let

$$\chi(p_i) = a^{m_i} .$$

Since $\alpha_1 = 2p_1 - p_2$

$$a^{\frac{q-1}{2}} = -1 = \chi(\alpha_1) = a^{2m_1} . a^{-m_2} .$$

Therefore m_2 is odd. Now $\chi(\alpha_3) = \chi(-p_2 + 2p_3 - p_4)$ implies that $\chi(-p_4)$ hence $\chi(p_4)$ is an odd power of a. Proceeding inductively we get that m_{2k} is odd for $k = 1, \ldots, [\frac{\ell-1}{2}]$.

If ℓ is odd, then $m_{\ell-1}$ is odd. But then $1 = \chi(\alpha_\ell) = \chi(-p_{\ell-1}+\ell p_\ell)$ gives

$$\chi(+p_{\ell-1}) = \chi(2p_\ell)$$

i.e. $$\alpha^{m_{\ell-1}} = a^{2m_\ell}$$

i.e. $$m_{\ell-1} \equiv 2m_\ell \pmod{q-1}$$

which is a contradiction.

If $\ell > z$ is even, then we have $m_{\ell-2}$ odd. But $\chi(\alpha_{\ell-1}) = 1 = \chi(-p_{\ell-2} + 2p_{\ell-1} - 2p_\ell)$

i.e. $$m_{\ell-2} \equiv 2(m_{\ell-1} - m_\ell) \pmod{q-1}$$

which is again a contradiction.

For $\ell = 2$ we have $-1 = a^{2(m_1 - m_2)}$ which is impossible.

Hence χ is a "non-extendable" homomorphism of P_r into K^*.

This proves our lemma.

The following lemma shows that we cannot expect a similar result when $|K| \equiv 1 \pmod 4$.

Lemma 6.4

If $|K| \equiv 1 \pmod 4$ then each character χ of P_r of order two can be extended to a character of P.

Proof.

Since $(\frac{q-1}{2})$ is now an even number and χ is of order two, the $\chi(\alpha_i)$ are even powers of a (i.e. either 1 or $a^{(q-1)/2}$). Let

$$\chi(\alpha_i) = a^{2m_i} ; \quad i = 1, 2, \ldots, \ell .$$

Then the character η of P_r defined by

$$\eta(\alpha_i) = a^{m_i}$$

satisfies

$$\eta^2 = \chi .$$

But $|\hat{H} : H| = 2$. Hence η^2 is always an extendable character.

Hence χ is an extendable character.

This proves our lemma.

§ (II) The Groups of Type C_ℓ . $\ell \geq 2$.

The Cartan Matrix is

$$A = (A_{ij}) = \begin{bmatrix} 2 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & \cdots & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 2 & -2 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & -1 & 2 \end{bmatrix}$$

In this case

(6.5) $\hat{D}/D \cong \hat{\mathfrak{h}}/\mathfrak{h} \cong \hat{H}/H$; $|\hat{H}/H| = 2 = |P/P_r|$

if $|K|$ is odd.

Also

$$\alpha_j = \sum_{i=1}^{\ell} A_{ij} \cdot p_i$$

gives

(6.6) $$\alpha_1 = 2p_1 - p_2$$

$$\alpha_2 = -p_1 + 2p_2 - p_3$$

$$\alpha_3 = -p_2 + 2p_3 - p_4$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\alpha_{\ell-1} = -p_{\ell-2} + 2p_{\ell-1} - p_\ell$$

$$\alpha_\ell = -2p_{\ell-1} + 2p_\ell \ .$$

Since $2p_i \in P_r \ \forall \ i$ as $|P/P_r| = 2$;

We have $p_2, \ p_4, \ p_6, \ \cdots \ \in P_r$

and $p_1, \ p_3, \ p_5, \ \cdots \ \notin P_r$.

Here again there is no non-trivial symmetry for the Dynkin diagram. The complement C' for D in $\hat{D}$ defined in the following lemma is sufficient for the construction of a complement for $\mathrm{Inn}\,(G)$ in $\mathrm{Au}(G)$.

Lemma 6.7

If $|K| \equiv 3 \pmod 4$ then D has a complement C' in $\hat{D}$.

Proof.

Define a character χ of P_r such that

$$\chi(a_\ell) = -1 \ ; \quad \chi(a_i) = 1 \ ; \qquad i \neq \ell \ .$$

Since $q \equiv 3 \pmod 4$; $q = |K|$, $(q-1)$ is even and $(\frac{q-1}{2})$ is odd. Hence an even power of a cannot be equal to an odd power of a . If χ were extendable to a character of P then let

$$\chi(p_i) = a^{m_i} \ .$$

Since $\alpha_\ell = -2p_{\ell-1} + 2p_\ell$ we have

$$-1 = \chi(\alpha_\ell) = \chi(-2p_{\ell-1} + 2p_\ell) .$$

Hence

$$a^{\frac{q-1}{2}} = a^{2(m_\ell - m_{\ell-1})} .$$

This contradicts $(\frac{q-1}{2})$ odd. χ is therefore non-extendable.

Hence

$$C' = < d(\chi) >$$

is obviously a complement for D in $\widehat{D}$, and the lemma is proved.

Remark (6.8)

The conclusion of the lemma does not hold for $|K| \equiv 1 \pmod 4$. This can be easily seen as in Lemma 7.4 .

§ (III) The Groups of Type E_7 .

The Cartan Matrix is

$$A = (A_{ij}) = \begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 2 \end{bmatrix}$$

Here

(6.9) $\quad \widehat{D}/D \cong \widehat{h}/h \cong \widehat{H}/H \; ; \qquad |\widehat{H/H}| = 2 = |P/P_r|$

if $|K|$ is odd.

Hence $\alpha_j = \sum_{i=1}^{\ell} A_{ij} \cdot p_i$ gives

(6.10)
$$\begin{aligned}
\alpha_1 &= 2p_1 - p_2 \\
\alpha_2 &= -p_1 + 2p_2 - p_3 \\
\alpha_3 &= -p_2 + 2p_3 - p_4 \\
\alpha_4 &= -p_3 + 2p_4 - p_5 - p_7 \\
\alpha_5 &= -p_4 + 2p_5 - p_6 \\
\alpha_6 &= -p_5 + 2p_6 \\
\alpha_7 &= -p_4 + 2p_7 \quad .
\end{aligned}$$

As $|P/P_r| = 2$ we can easily see that

$$p_2, p_4, p_5, p_6 \in P_r$$

and p_1 , p_3 and $p_7 \notin P_r$.

There is no non-trivial symmetry of the Dynkin diagram.

<u>Lemma (6.11)</u>

If $|K| \equiv 3 \pmod 4$ then there is a complement C' for D in $\hat{D}$.

<u>Proof</u>.

Let χ be the character of P_r with

$$\chi(\alpha_1) = -1 \ ; \quad \chi(\alpha_i) = 1 \ , \quad i \neq 1 \ .$$

$q-1$ is even and $(\frac{q-1}{2})$ is odd where $q = |K|$. If χ were extendable to a character of P let $K^* = < a >$ and $\chi(p_i) = a^{m_i}$. Then

$$\chi(\alpha_1) = \chi(2p_1) \cdot \chi(-p_2)$$

shows that m_2 is odd, as $(\frac{q-1}{2})$ is odd. Hence m_4 is odd, because of

$$\chi(\alpha_3) = \chi(-p_2)\ \chi(2p_3)\ \chi(-p_4) \ .$$

But

$$\alpha_7 = -p_4 + 2p_7 \ \text{ gives}$$

$$\chi(p_4) = \chi(2p_1) \ \text{ i.e.}$$

$$m_4 \equiv 2m_7 \pmod{q-1}$$

which is a contradiction as m_4 is odd.

χ therefore is a non-extendable character of P_r. The group

$$C' = < d(\chi) >$$

is a complement for D in $\hat{D}$.

Remark 6.12

D has no complement in $\widehat{D}$ when $|K| \equiv 1 \pmod 4$.

§ (IV) The Groups of Type E_6 .

The Cartan matrix for E_6 is

$$A = (A_{ij}) = \begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 \end{bmatrix}$$

(6.13) $\widehat{D}/D \cong \widehat{\mathfrak{h}}/\mathfrak{h} \cong \widehat{H}/H$; $|\widehat{H}/H| = 3 = |P/P_r|$

if $|K| \equiv 1 \pmod 3$.

Now

$$\alpha_1 = \sum_{i=1}^{\ell} A_{ij} \cdot p_i \quad \text{gives}$$

(6.14) $\alpha_1 = 2p_1 - p_2$

$\alpha_2 = -p_1 + 2p_2 - p_3$

$\alpha_3 = -p_2 + 2p_3 - p_4 - p_6$

$\alpha_4 = -p_3 + 2p_4 - p_5$

$$\alpha_5 = -p_4 + 2p_5$$

$$\alpha_6 = -p_3 + 2p_6 \ .$$

Since $|P/P_r| = 3$; p_3 and $p_6 \in P_r$ whereas $p_1 , p_2 , p_4 , p_5 \notin P_r$.

For the Dynkin diagram of E_6 there is a non-trivial symmetry; viz

$$\alpha_6 \rightarrow \alpha_6 \quad \text{and}$$

$$\alpha_i \rightarrow \alpha_{6-i} \ ; \quad i \leq 5 \ .$$

In this case we have the following

<u>Lemma 6.15</u>

If $q \equiv 1 \pmod 3$, $q = |K|$, then the condition that " D has a complement C' in $\hat{D}$ such that for any summetry φ of the Dynkin diagram and for $\chi \in C'$ the composition $\chi o \ \varphi \in C'$ " holds if and only if $\frac{q-1}{3} \not\equiv 0 \pmod 3$.

<u>Proof.</u>

Since $|\widehat{D}/D| = 3$ if D has a complement C' in $\hat{D}$ then $|C'| = 3$; i.e. C' must be generated by an element $d(\chi)$ of $\hat{D}$ such that

$$\chi(\alpha_i) = a^{m_i} \ ; \ K = < a > \ ,$$

where the m_i are multiples of $(\frac{q-1}{3})$. i.e.

$$3 \ m_i \equiv 0 \ (\text{mod } q-1) \ .$$

Also if φ is the non-trivial symmetry

$$\varphi : \alpha_6 \to \alpha_6$$

$$\alpha_i \to \alpha_{6-i} ; \quad i \leq 5$$

then the condition requires that

$$\chi \circ \varphi \in C' \quad \text{i.e.}$$

$$\chi \circ \varphi = \chi \quad \text{or} \quad \chi^2$$ ($\chi \circ \varphi$ can never be 1 if $\chi \neq 1$). This means

$$\chi(\varphi(\alpha_i)) = \chi(\alpha_i) \qquad i = 1, \ldots, 6$$

$$\text{or} \qquad = \chi^2(\alpha_i) \qquad i = 1, \ldots, 6$$

i.e.

(1) $m_1 \equiv m_5$

(2) $m_2 \equiv m_4$

and

(3) m_3 and m_6 arbitrary.

or

(1) $2m_1 \equiv m_5$

(2) $2m_2 \equiv m_4$

and

(3) $m_3 \equiv m_6 \equiv 0$.

Let η be a mapping of P into K^* such that

$$\eta(\alpha_i) = \chi(\alpha_i) \quad \text{and}$$

$$\eta(p_1) = a^{K_1} \quad ; \qquad \eta(p_6) = a^{K_2} \quad .$$

We suppose that η is a homomorphism of P into K^* (and hence an extension of the character χ to a character of P). Then

$$\eta(\alpha_1) = \eta(2p_1 - p_2)$$

$$\eta(\alpha_1) = (\eta(p_1))^2 \, (\eta(p_2))^{-1}$$

i.e.

$$a^{m_1} = a^{2K_1} \cdot (\eta(p_2))^{-1}$$

i.e.

$$\eta(p_2) = a^{2K_1 - m_1} .$$

Similarly we must have

$$\eta(p_3) = a^{3K_1 - 2m_1 - m_2}$$

$$\eta(p_4) = a^{4K_1 - 3m_1 - 2m_2 - m_3 - K_2}$$

$$\eta(p_5) = a^{5K_1 - 4m_1 - 3m_2 - 2K_2 - 2m_3 - m_4} .$$

Now

$$\eta(\alpha_5) = \chi(\alpha_5) = \eta(-p_4 + 2p_5)$$

i.e. $$a^{m_5} = a^{6K_1 - 5m_1 - 4m_2 - 3K_2 - 2m_4 - 3m_3}$$

i.e. $$m_5 \equiv 6K_1 - 5m_1 - 4m_2 - 3m_3 - 3K_2 - 2m_4$$ and

$$\eta(a_6) = \chi(a_6) = \eta(-p_3 + 2p_6)$$

gives us

$$m_6 \equiv 2K_2 - 3K_1 + 2m_1 + m_2 .$$

The last two equations give us conditions on K_1 and K_2 .

$$K_2 \equiv m_1 + 2m_2 + 3m_3 + 2m_4 + m_5 + 2m_6$$

and

$$3K_1 \equiv 4m_1 + 5m_2 + 6m_3 + 4m_4 + 2m_5 + 3m_6 \ .$$

Since $3m_i \equiv 0 \pmod{q-1}$

$$K_2 \equiv m_1 + 2m_2 + 2m_4 + m_5 + 2m_6$$

and

$$3K_1 \equiv 4m_1 + 5m_2 + 4m_4 + 2m_5 \ .$$

<u>Case 1</u> $\chi \circ \varphi = \chi$.

Hence $m_1 \equiv m_5$, $m_2 \equiv m_4$ and m_3 and m_6 are arbitrary.

$$\therefore \quad K_2 \equiv 2m_1 + 4m_2 + 2m_6$$

and $3K_1 \equiv 0$.

Hence, in this case K_2 and K_1 can be chosen modulo $(q-1)$ such that they satisfy the last two conditions and hence η with these values of K_1 and K_2 can be extended to a homomorphism of P into K^* i.e. χ is extendable.

<u>Case 2</u> $\chi \circ \varphi = \chi^2$. Here $2m_1 \equiv m_5$, $2m_2 \equiv m_4$, $m_3 \equiv m_6 \equiv 0$. Equivalently $m_1 \equiv 2m_5$, $m_2 \equiv 2m_4$ and $m_6 \equiv m_3 \equiv 0$. Then

$$K_2 \equiv 0 \quad \text{and}$$

$$3K_1 \equiv 2m_1 + m_2 \ .$$

The last equation is important.

Suppose $\frac{q-1}{3} \equiv 0 \pmod 3$; then $K_1 \equiv (\frac{2m_1 + m_2}{3})$ can be satisfied since 3 divides $\frac{q-1}{3}$ which divides m_1 and m_2, hence $2m_1 + m_2$. Hence taking appropriate values of K_1 and K_2 we get a homomorphism of P into K^* which extends χ.

This means that if $\frac{q-1}{3} \equiv 0 \pmod 3$ then any character χ of P_r such that

" $\chi^3 = 1$ and $\chi \circ \varphi$ is χ^2 or χ "

is extendable. Hence $d(\chi) \in D$. So D has no complement in $\widehat{D}$ if $\frac{q-1}{3} \equiv 0 \pmod 3$.

On the other hand if $\frac{q-1}{3} \not\equiv 0 \pmod 3$ take $m_1 = \frac{q-1}{3} = m_4$ and $m_2 = 2(\frac{q-1}{3}) = m_5$. Then if η is an extension of χ and if $\eta(p_1) = a^{K_1}$ we must have

$$3K_1 \equiv 2(\frac{q-1}{3}) + 2(\frac{q-1}{3})$$

i.e.
$$3K_1 \equiv (\frac{q-1}{3})$$

i.e.
$$3 \text{ divides } (\frac{q-1}{3})$$

which is a contradiction. Hence χ has no extension. Hence in this case (i.e. when $\frac{q-1}{3} \not\equiv 0 \pmod 3$)

$C' = < d(\chi) >$, where $\chi(\alpha_1) = a^{(q-1)/3}$, $\chi(\alpha_2) = a^{2(q-1)/3}$ and $\chi(\alpha_i) = 1$, $i \neq 1, 2$, is a complement for D in $\widehat{D}$ with

$$\chi \circ \varphi = \chi^2 \; .$$

This proves our lemma.

§ (V) The Groups of the Type D_ℓ , $\ell \geq 4$.

The Cartan Matrix is

$$A = (A_{ij}) = \begin{bmatrix} 2 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 2 & -1 & -1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & -1 & 0 & 2 \end{bmatrix}$$

Hence $\alpha_j = \sum_{i=1}^{\ell} A_{ij} \cdot p_i$ gives

(6.16) $$\alpha_1 = 2p_1 - p_2 \; .$$

$$\alpha_2 = -p_1 + 2p_2 - p_3$$

$$\alpha_3 = -p_2 + 2p_3 - p_4$$

$$\cdot = \cdot \quad \cdot \quad \cdot$$

$$\alpha_{\ell-3} = -p_{\ell-4} + 2p_{\ell-3} - p_{\ell-2}$$

$$\alpha_{\ell-2} = -p_{\ell-3} + 2p_{\ell-2} - p_{\ell-1} - p_\ell$$

$$\alpha_{\ell-1} = -p_{\ell-2} + 2p_{\ell-1}$$

$$\alpha_\ell = -p_{\ell-2} + 2p_\ell \ .$$

Case (1) $\quad \ell$ even

(6.17) $\quad \hat{D}/D \cong \hat{\mathfrak{L}}/\mathfrak{L} \cong \hat{H}/H \ ; \quad |\hat{H}/H| = 4$

if $|K| = p^n$ is odd. P/P_r is a Four group.

Hence $2p_i \in P_r \ \forall \ i$. We have

$$p_2, p_4, p_6, \ldots, p_{\ell-2} \in P_r$$

and

$$p_1, p_3, p_5, \ldots, p_{\ell-3}, p_{\ell-1}, p_\ell \notin P_r$$

Lemma (6.18)

$\hat{H}/H$ is a Four group.

Proof

Let χ be any character of P_r . We show that χ^2 is an extendable character.

Since $(2p_i) \in P_r$ for all i , $\chi(2p_i)$ is well defined. Define a mapping η of P into K^* such that $\eta(p_i) = \chi(2p_i)$.

Since $\{p_1, p_2, \ldots, p_\ell\}$ is a basis for P, η can be extended to a homomorphism of P. Since χ is a homomorphism of P_r into K^* it can be easily seen that

$$\eta(\alpha_i) = (\chi(\alpha_i))^2 \quad \text{for all } i$$

i.e. $$\eta = \chi^2 \quad \text{on } P_r$$

and χ^2 can be extended to a homomorphism (viz η) of P into K^*.

This proves the lemma.

We now prove the following:

<u>Lemma (6.19)</u>

If $|K| = p^n \equiv 3(\mathrm{mod}\ 4)$ then there is a complement C' for D in $\widehat{D}$ such that if φ is the non-trivial symmetry of the Dynkin diagram then $d(\chi \circ \varphi) \in C'$ whenever $d(\chi) \in C'$.

<u>Proof</u>.

As usual we shall construct this complement C'. First suppose $\ell \neq 4$.

We define two characters χ_1 and χ_2 of P_r as follows:

$$\chi_1(\alpha_\ell) = -1 \ ; \quad \chi_1(\alpha_i) = 1 \ , \quad i \neq \ell \ .$$

$$\chi_2(\alpha_{\ell-1}) = -1 \ ; \quad \chi_2(\alpha_i) = 1 \ , \quad i \neq \ell-1 \ .$$

Since $q \equiv 3 \ (\mathrm{mod}\ 4)$, $(q-1)$ is even. Hence an odd power of a where $< a > = K^*$ cannot be equal to an even power of a. Also

$-1 = a^{(q-1)/2}$ where $(\frac{q-1}{2})$ is an odd number. Note that for the three characters χ_1 , χ_2 and $(\chi_1 \cdot \chi_2)$ we have

$$\chi_1^2 = \chi_2^2 = (\chi_1 \cdot \chi_2)^2 = 1 .$$

We want to show that none of χ_1, χ_2 or $(\chi_1 \cdot \chi_2)$ can be extended to a character of P . Suppose the contrary and let χ denote any one of χ_1, χ_2 or $(\chi_1 \cdot \chi_2)$; and let

$$\chi(p_i) = a^{m_i} .$$

We first note that $m_{\ell-2}$ is always an odd number. This, in turn makes $m_{\ell-4}$, $m_{\ell-6}$, ..., m_2 odd. But

$$\chi(\alpha_1) = \chi(2p_1 - p_2)$$

gives

$$m_2 \equiv 2m_1 \pmod{q-1}$$

i.e. m_2 is even.

The contradiction proves our result. Hence non of χ_1, χ_2 or $\chi_1 \cdot \chi_2$ is an extendable character. Hence $d(\chi_1)$, $d(\chi_2)$ and $d(\chi_1 \cdot \chi_2)$ are not in D . In fact

$$C' = \{d(\chi_1), d(\chi_2), d(\chi_1 \cdot \chi_2), 1\}$$

is a complement for D in $\widehat{D}$. Finally note that

$$\chi_1 \circ \varphi = \chi_2$$

$$\chi_2 \circ \varphi = \chi_1$$

$$(\chi_1 \cdot \chi_2) \circ \varphi = \chi_1 \cdot \chi_2 \quad .$$

Hence our lemma is proved for $\ell \neq 4$.

In the case $\ell = 4$, the C' defined above does give a complement for D in $\widehat{D}$, but the problem here is that the group of symmetries of the corresponding Dynkin diagram is isomorphic to the symmetric group $S(3)$ on three elements. Any permutation of α_1 , α_3 and α_4 gives a symmetry. If φ is the transposition (α_4, α_1) then $d(\chi_1) \in C'$ but $d(\chi_1 \cdot \varphi) \notin C'$.

But in this case the following three characters work.

Define χ_1, χ_2 and χ_3 such that

$$\chi_1(\alpha_1) = \chi(\alpha_3) = -1 \ ; \quad \chi(\alpha_2) = \chi(\alpha_4) = 1 \ .$$

$$\chi_2(\alpha_1) = \chi_2(\alpha_4) = -1 \ ; \quad \chi_2(\alpha_2) = \chi_2(\alpha_3) = 1 \ .$$

and

$$\chi_3(\alpha_3) = \chi_3(\alpha_4) = -1 \ ; \quad \chi_3(\alpha_2) = \chi_3(\alpha_1) = 1 \ .$$

Then it is easily seen that χ_1, χ_2 and χ_3 are non-extendable characters such that

$$\chi_1^2 = \chi_2^2 = 1 \quad \text{and} \quad \chi_1\,\chi_2 = \chi_2 \cdot \chi_1 = \chi_3 \,.$$

Also for each $i = 1, 2, 3$, $\chi_i \circ \varphi = \chi_j$ for some $j = 1, 2, 3$ where φ is a symmetry.

$$C' = \{1, d(\chi_1), d(\chi_2), d(\chi_3)\}$$

is therefore a complement of the required type when $\ell = 4$.

This proves our lemma.

Remark (6.20)

When $q \equiv 1 \pmod{4}$, $q \equiv |K|$ then $(\frac{q-1}{2})$ is an even number. Hence if χ is any character of P_r such that $\chi^2 = 1$ then we can (see e.g. Lemma 6.4) define a character η of P_r such that $\eta^2 = \chi$. But by Lemma (6.18), for any character η of P_r, η^2 is always extendable to a character of P . This means we cannot find a complement for D in D .

Case (2) D_ℓ with ℓ odd. In this case

(6.21) $D/D \cong \;\; /\,h' \cong H/H$ with

$$|H/H| = 2 \quad \text{if} \quad |K| \equiv 3 \pmod{4}$$

$$= 4 \quad \text{if} \quad |K| \equiv 1 \pmod{4} \,;$$

and P/P_r is a cyclic group of order 4 .

Then

$p_2, p_4, p_6, \ldots, p_{\ell-3} \in P_r$ and $pi \notin P_r$ otherwise.

Also $2p_1, 2p_3 \ldots 2p_{\ell-2}$, $4p_{\ell-1}, 4p_{\ell-1}, 4p_\ell \in P_r$ and $(p_{\ell-1} + p_\ell) \in P_r$.

We now prove the following:

Lemma (6.22)

If χ is a character of P_r of order two and such that

$\chi(\alpha_{\ell-1}) = \chi(\alpha_\ell)$ then χ can be extended to a character of P .

Proof

Define a character η of P as follow.

Let $\eta(p_{\ell-2}) = \chi(\alpha_\ell) = \chi(\alpha_{\ell-1})$

Then define, successively

$$\eta(p_{\ell-4}) = \chi(\alpha_{\ell-3})\, \eta(p_{\ell-2}) ,$$

$$\eta(p_{\ell-6}) = \chi(\alpha_{\ell-5})\, \eta(p_{\ell-4}) ,$$

$$\cdots\cdots = \cdots \quad \cdots\cdots ,$$

$$\eta(p_3) = \chi(\alpha_4)\, \eta(p_5) ,$$

$$\eta(p_1) = \chi(\alpha_2)\, \eta(p_3) .$$

Let $\eta(p_2) = \chi(\alpha_1)$,

$$\eta(p_4) = \chi(\alpha_3)\, \eta(p_2) ,$$

$$\eta(p_6) = \chi(\alpha_5)\, \eta(p_4) ,$$

$$\cdots = \cdots \quad \cdots ,$$

$$\eta(p_{\ell-3}) = \chi(\alpha_{\ell-4})\, \eta(p_{\ell-5}) .$$

Finally take

$$\eta(p_{\ell-1}) = \chi(\alpha_{\ell-2}) \quad \text{and} \quad \eta(p_\ell) = 1 .$$

Since $\chi(\alpha_i)$ are $+1$ or -1 η can be easily seen to be an extension of χ.

This proves the lemma.

With the above result we are now in a position to prove

Lemma (6.23)

For groups of type D_ℓ, ℓ odd ; there is no complement C' for D in $\hat{D}$ which satisfies the condition $d(\chi \circ \varphi) \in C'$ for every symmetry φ and every $\chi \in C'$.

Proof

Suppose the contrary and let C' be of given type. Then C' is either a Four group or a cyclic group of order four. Let $\chi \in C'$, χ of order two. Since the only non-trivial symmetry φ is the one which interchanges $\alpha_{\ell-i}$ and α_ℓ, we see that $(\chi \circ \varphi)$ is of order two. If $\chi = \chi \circ \varphi$ then $\chi(\alpha_\ell) = \chi(\alpha_{\ell-1})$. If $\chi \neq \chi \circ \varphi$ then C' must be the Four group, and hence $\eta = \chi(\chi \circ \varphi)$ is of order two. But now $\eta(\alpha_\ell) = \chi(\alpha_\ell)\,\chi(\alpha_{\ell-1}) = \eta(\alpha_{\ell-1})$. In both cases we get a character Ψ of order two which can not be extended to P and which satisfy the relation $\Psi(2_\ell) = \Psi(2_{\ell-1})$. This is a contradiction in view of lemma (6.22). Hence there is no complement C' of required type, and the lemma is proved.

§ (VI) The Groups of the Type A_ℓ, $\ell \geq 1$.

The Cartan Matrix is

$$A = (A_{ij}) = \begin{bmatrix} 2 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & \cdots & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 2 \end{bmatrix}$$

We get

$$\alpha_1 = 2p_1 - p_2$$

$$\alpha_2 = -p_1 + 2p_2 - p_3$$

$$\alpha_3 = -p_2 + 2p_3 - p_4$$

$$\cdot \quad \cdot \qquad \cdot \quad \cdot$$

$$\alpha_{\ell-1} = -p_{\ell-2} + 2p_{\ell-1} - p_\ell$$

$$\alpha_\ell = -p_{\ell-1} + 2p_\ell \ .$$

and

(6.25) $$\widehat{D}/D \cong \hat{h}/h \cong \hat{H}/H \ ;$$

$$|\hat{H}/H| = d = \text{g.c.d.} \ (\ell+1, \ |K| - 1) \ ;$$

and

$$P/P_r \text{ is cyclic of order } \ell+1 \ .$$

Since we have already considered the case $d = 1$ (see Lemma 3.6) we assume that $d > 1$.

We now prove the following:

Lemma (6.26)

Let $q-1 = d.u.$ Let either (1) d odd and g.c.d. $(d,u) = 1$ or (2) $\ell+1 \equiv q-1 \equiv 2 \pmod 4$.

Then D has a complement C' in $\widehat{D}$ such that the following condition is satisfied:

" $d(\chi \circ \varphi) \in C'$ for every symmetry φ and for all $d(\chi) \in C'$. "

Proof

Let χ be a character of P_r such that if d is an odd number then

$$\chi(\alpha_1) = a^{(q-1/d)} \quad ; \quad \chi(\alpha_\ell) = a^{c(q-1/d)}$$

$$\text{and} \quad \chi(\alpha_i) = 1 \quad ; \quad i \neq 1, \ell ,$$

where c is an integer between 1 and d to be specified later. If d is even then ℓ is odd and we put

$$\chi(\alpha + 1/2) = -1 \; ; \; \chi(\alpha_i) = 1 \; ; \; i \neq \left(\frac{\ell+1}{2}\right) .$$

We shall show that χ^i is not extendable to a character of P_r for $i \leq i < d$.

Suppose the contrary and let $\chi^i(p_1) = a^{K_1}$. If we are in the case where d is an odd number then

$$\chi^i(\alpha_1) = a^{i(q-1/d)} = \chi^i(2p_1 - p_2)$$

and hence

$$\chi^i(p_2) = a^{2K_1 - i(q-1/d)}$$

Similarly

$$\chi^i(p_3) = a^{3K_1 - 2i(q-1/d)} \quad ; \quad \chi^i(p_4) = a^{4K_1 - 3i(q-1/d)} ,$$

etc. up to

$$\chi^i(p_\ell) = a^{\ell K_1 - i(\ell-1)(q-1/d)} .$$

Hence

$$\chi^i(\alpha_\ell) = a^{ic(q-1/d)} = a^{(\ell+1)K_1 - \ell i(q-1/d)}$$

i.e. $\quad (\ell+1)K_1 - i(\ell+c)(q-1/d) \equiv 0 \pmod{q-1}$,

and hence

$$(\ell+1)(K_1 - i(q-1/d)) - (c-1)i \cdot (q-1/d) = u.d.m.$$

for some integer m . So $(\ell+1)(K_1 - iu) - i(c-1)\, u = u.d.m.$

Since d divides $\ell+1$ and g.c.d. $(d,u) = 1$, d divides $i \cdot (c-1)$.

Take $c = (d-1)$. Now $(c-1) = (d-2)$ and d are relatively prime as d is an odd number. Hence d divides i where $i = 1, 2, 3, \ldots, (d-1)$. This contradiction shows that with this $c = (d-1)$ χ^i is not extendable for $i = 1, 2, 3, \ldots, d-1$. In other words

$$C' = < d(\chi) > , \quad d(\chi)^d = 1$$

is a complement for D in $\widehat{D}$. We now show that C' is, in fact a complement of the desired type.

Let φ be the symmetry given by

$$\alpha_i \to a_{\ell+1-i} \quad . \quad i = 1, 2, 3, \ldots, \ell \quad .$$

Then

$$\chi \circ \varphi (\alpha_1) = \chi(\alpha_\ell) = a^{c(q-1/d)} = \chi(\alpha_1)^c$$

$$\chi \circ \varphi (\alpha_i) = 1 = \chi(\alpha_i) \; ; \quad i \neq 1, \ell ,$$

and

$$\chi \circ \varphi \;(\alpha_\ell) = \chi(\alpha_1) = a^{(q-1/d)} \quad .$$

But $c = d-1$ gives

$$c^2 \equiv 1 \pmod d$$

$$\therefore \quad c^2 . \left(\frac{q-1}{d}\right) \equiv \left(\frac{q-1}{d}\right) \pmod{(q-1)} \quad .$$

Hence

$$\chi \circ \varphi (\alpha_\ell) = a^{q-1/d} = (a^{c(q-1/d)})^c$$

$$= (\chi(\alpha_\ell))^c$$

i.e. $\qquad \chi \circ \varphi = \chi^c \quad .$

This proves the lemma for odd d .

If d is even then $\chi(p_1) = a^{K_1}$ and $\chi(\alpha_1) = 1 = \chi(2p_1 - p_2)$ gives

$\chi(p_2) = a^{2K_1}$. Similarly $\chi(p_3) = a^{3K_1}$, $\chi(p_4) = a^{4K_1}$, etc., to

$\chi(p_{\frac{\ell+1}{2}}) = a^{(\ell+1/2)K_1}$. Since $\chi(\alpha_{\frac{\ell+1}{2}}) = -1 = \chi(-p_{\frac{\ell-1}{2}} + 2p_{\frac{\ell+1}{2}} - p_{\frac{\ell+3}{2}})$

we have

$$\chi(p_{\frac{\ell+3}{2}}) = (-1) \cdot a^{\ell+3/2} \cdot K_1$$
$$= a^{(\ell+3/2 \,.\, K_1 + q-1/2)} \,.$$

Finally

$$\chi(p_\ell) = a^{(\ell K_1 + \ell-1/2 \,.\, q-1/2)} \,.$$

Hence $\chi(\alpha_\ell) = 1 = \chi(2p_\ell - p_{\ell-1})$ gives

$$a^{(\ell+1)K_1 + \ell+1/2 \,.\, q-1/2} = 1 \,.$$

i.e. $\quad (\ell+1)K_1 \equiv \frac{\ell+1}{2} \cdot \frac{q-1}{2} \pmod{q-1}$.

Since $(\ell+1)$ and $(q-1)$ are even, $(\frac{q-1}{2})(\frac{\ell+1}{2})$ is even which is a contradiction as $\frac{q-1}{2}$ and $(\frac{\ell+1}{2})$ are odd.

Hence χ is a non-extendable character of P_r .

Finally for the non-trivial symmetry φ

$$\varphi(\alpha_{\frac{\ell+1}{2}}) = \alpha_{\frac{\ell+1}{2}}$$

Hence $\chi \circ \varphi = \hat{\chi}$.

Take

$$C' = \langle d(\chi) \rangle \,, \quad d(\chi)^2 = 1$$

and the lemma is proved for even d .

§ (VII) Beyond the sufficient condition.

If Inn (G) has a complement C in Au(G) then for an element

$$\sigma \in C \cap \hat{D} I \qquad \text{we have}$$

$$\sigma = u_1^* \, d(\chi) \, . \, \omega(w)^* \, u_2^*$$

where x^* denotes the inner automorphism of G corresponding to $x \in G$. (see proposition 1.23).

In the sufficient condition we looked for those $\sigma \in C \cap \hat{D} I$ which are in fact in $\hat{D}$. Presently we shall look for more general type of $\sigma \in C \cap \hat{D} I$; viz of the form

$$\sigma = d(\chi) \, . \, \omega(w)^* \, .$$

In the case of groups of type B_ℓ, C_ℓ and E_7 the complement C for I in Au(G) is obtained in cases which does not satisfy the sufficient condition.

In fact we have the following

Theorem (6.27)

Suppose we are in the case B_ℓ, C_ℓ or E_7 and further suppose p is an odd prime and

$$|K| = q = p^n \; ; \quad n = \text{an odd number.}$$

Then Inn (G) has a complement C in Au (G).

(Note that here we do not require $q \equiv 3 \pmod 4$).

Proof

Note that

$$q-1 = p^n-1 = (p-1)(p^{n-1} + \ldots + p + 1) \quad .$$

Since n is odd and p is an odd prime $(1 + p + p^2 + \ldots p^{n-1})$ is odd . If $|r|_2$ denotes the maximum power of 2 which divides the integer r then

$$|q-1|_2 = |p-1|_2 = m' \quad , \text{ say, and let } m = \frac{q-1}{m'} \quad .$$

Let us now define a character χ of P_r as follows:

If the groups are of the type B_ℓ or E_7 define χ such that

$$\chi(\alpha_1) = a^m \; ; \quad \chi(\alpha_i) = 1 \; , \; i \neq 1 \; .$$

For C_ℓ let $\chi(\alpha_\ell) = a^m \; ; \quad \chi(\alpha_i) = 1 \; , \; i \neq 1 \; .$

Since m is an odd number it can be seen that χ defined in each case above cannot be extended to a character of P .

Now by (2.1, [5]) there is an element w in the Weyl group W such that

$$w(\alpha_i) = -\alpha_i \quad \text{for all } i \; .$$

Let $\omega(w) \in \overline{W}$ such that $\zeta(\omega(w)) = w$ (here ζ is the map of p. 15, 1.21). We can select $\omega(w)$ such that

$$\omega(w) = \prod_r \cdot \; \omega_r \quad .$$

For any root r , since $w^2 = 1$

$$x_r(t)^{\omega(w)^2} = x_{w(r)}(\eta_r t)^{\omega(w)}$$

$$= x_{w^2(r)}(\eta_{w(r)}\eta_r t)$$

$$= x_r(\eta_{-r}\eta_r t)$$

If $\{e_r : r \in R \,;\, h_r : r \in \pi\}$ is a Chevalley basis then

$$\omega(w)(e_s) = (\prod_r \omega_r)(e_s)$$

$$= (\prod_r \eta_s^r)\, e_{w(s)} \quad ; \quad (\text{cf. } 1.17)$$

where η_s^r corresponds to ω_r . Hence

$$\eta_s = \prod_r \cdot \; \eta_s^r$$

Finally for any roots s and r ,

$$\omega_r X_s = \eta_s^r \; X_{w_r(s)}$$

$$\omega_r X_{-s} = \eta_{-s}^r \; X_{w_r(-s)} \; .$$

$$\therefore \quad \omega_r[X_s \; X_{-s}] = \eta_s^r \; \eta_{-s}^r \; [X_{w_r(s)} \, , \, X_{-w(s)}]$$

$$\therefore \quad \omega_r \; h_r = \eta_s^r \; \eta_{-s}^r \; h_{w_r(s)} \quad ; \quad (\S\, \text{III, Ch. } 1)$$

$$\therefore \quad h_{w_r(\;)} = \eta_s^r \; \eta_{-s}^r \; h_{w_r(s)}$$

$$\therefore \quad \eta_s^r \; \eta_{-s}^r = 1 \; .$$

$$\therefore \quad (\prod_r \eta_s^r)(\pi_r \; \eta_{-s}^r) = 1 \; .$$

Hence $\eta_s \cdot \eta_{-s} = 1$ and

$$x_r(t)^{\omega(w)^2} = x_r(\eta_r \; \eta_{-r} \; t)$$

$$= x_r(t)$$

for any root .

$$\therefore \quad \omega(w)^2 = 1 \; .$$

Hence with $C_1 = d(\chi)\; \omega(w)^*$ we have

$$c_1^2 = d(\chi) \; . \; \omega(w)^* \;\; d(\chi) \; . \; \omega(w)^*$$

$$= d(\chi) \; . \; \omega(w)^* \; d(\chi) \; (\omega(w)^*)^{-1}$$

$$= d(\chi) \; . \; d(\chi^{-1}) = d(\chi\chi^{-1}) = 1$$

Since

$$\chi(w(\alpha_i)) = \chi(-\alpha_i) = \chi^{-1}(\alpha_i) \quad \text{for} \quad i = 1, 2, \ldots, \ell \; .$$

Since χ is non-extendable $d(\chi) \not\in D$. Hence $c_1 = d(\chi)$. - - $\omega(w)^* \not\in \mathrm{Inn}\,(G)$. Now consider $f \cdot c_1 \cdot f^{-1}$ where f is the generator of the group of field automorphism group F of G . We have

$$fc_1f^{-1} = f.d(\chi).\; \omega(w)^* f^{-1} \; .$$

$$= (f.d(\chi)f^{-1})(f.\omega(w)^* f^{-1})$$

$$= (d(\chi^p))(\omega(w)^*)$$

But $(\chi(\alpha_j))^{p-1} = a^{m(p-1)}$, where $j = 1$ for B_ℓ or E_7 and $j = \ell$ for C_ℓ,

and
$$m(p-1) = \left(\frac{q-1}{|q-1|_2} \right)(p-1)$$
$$= \left(\frac{q-1}{|p-1|_2} \right)(p-1)$$
$$\equiv 0 \pmod{q-1} \ .$$

Hence $\chi^{p-1} = 1$ and $d(\chi^p) = d(\chi)$; i. e. $f.c_1f^{-1} = d(\chi) \cdot \omega(w)^* = c_1$.

$\therefore$ F centralizes the element c_1 . Let
$$C_1 = \langle c_1 \rangle \ ; \ c_1^2 = 1$$
and
$$C = \langle F \cdot C_1 \rangle .$$

It is now easy to see that C forms a complement for I in $Au(G)$.

CHAPTER 7

A SUFFICIENT CONDITION AND THE TWISTED TYPE GROUPS

§ (I) A sufficient condition.

Due to the similarity between the situation for the groups of Chevalley type and those of Twisted types, the sufficient condition developed for the Chevalley type can easily be modified for the groups of Twisted type. This is done in the following

Theorem (7.1)

Suppose D^1 has a complement C' in $\hat{D}^1$. Then

$$C = \langle C' \cup F \rangle$$

is a complement for $\mathrm{Inn}\,(G^1) = I$ in $\mathrm{Au}(G^1)$.

Proof

We saw (see § (V), Ch. 1) that elements of $\hat{D}^1$ are of the form $d(\chi)$ where χ is a self-conjugate character of P_r. We also noted (in the proof of theorem 5.1) that conjugation by $f \in F$ of an element $d(\chi)$ of $\hat{D}$ is obtained simply by taking the appropriate power of the same element; i.e.

$$f \cdot d(\chi) f^{-1} = d(\chi)^{p^i} .$$

Hence F normalizes C', and

$$C = \langle C' \cup F \rangle = F\,C' .$$

Let $x \in C \cap I\ \mathrm{Inn}\ (G^1)$ then

$$x = f \cdot d(\chi)\ ; \quad f \in F\ ,\ d(\chi) \in C' \quad \text{and}$$

$$x \in \mathrm{Inn}\ (G^1) .$$

This gives

$$1 = f \cdot d(\chi)\ x^{-1} .$$

and because of ([18])

we see that

$$f = 1\ ,\ \text{i.e.}$$

$$x = d(\chi)\ ; \quad x \in \mathrm{Inn}\ (G^1) .$$

But $d(\chi) \in C'$ where

$$C' \cap D^1 = 1\ ,$$

and

$$\hat{D}^1 \cap \mathrm{Inn}\ (G^1) = D^1 .$$

Thus we have

$$x = d(\chi) = 1 .$$

Hence

$$C \cap \mathrm{Inn}\ (G^1) = 1 .$$

Since G^1 has no "graph automorphism" (p. 614, [16]) it follows that C and $\mathrm{Inn}\ (G)$ generate $\mathrm{Au}(G)$.

This proves the theorem.

We shall now try to verify this condition for different Twisted types.

§ (II) The Groups of the Type E_6^1 .

In this case

(7.2) $\hat{D}^1/D^1 \cong \hat{h}^1/h^1 \cong \hat{H}^1/H^1$;

$$\left|\frac{\hat{H}^1}{H^1}\right| = d = \text{g.c.d.} \quad (3, r+1)$$

where $|K| = p^{2n} = r^2 = q$.

We prove the following

Lemma (7.3)

D^1 has a complement C' in $\hat{D}^1$ if

either (1) $r \not\equiv 2 \pmod 3$

or (2) $r \equiv 2 \pmod 3$

and $r^2 \not\equiv 1 \pmod 9$.

Proof

If $r \not\equiv 2 \pmod 3$ then $r + 1 \not\equiv 0 \pmod 3$ and hence d = g.c.d. $(3, r+1) = 1$.

i.e.

$D^1 = \hat{D}^1$ and the identity is a complement for D^1 in $\hat{D}^1$. Let $r \equiv 2 \pmod 3$ but $r^2 \not\equiv 1 \pmod 9$. Then d = g.c.d. $(3, r+1) = 3$. Let us define the character χ of P_r such that

$$\chi(\alpha_1) = a^{(r^2 - 1)/3} = \chi(\alpha_4)$$

$$\chi(\alpha_2) = a^{2(r^2 - 1)/3} = \chi(\alpha_5)$$

and $$\chi(\alpha_6) = 1 = \chi(\alpha_3) \; .$$

We saw in Lemma 6.15 that this character χ of P_r is not extendable to a character of P. Hence if we can show that

$$\chi(\varphi(\alpha_i)) = (\chi(\alpha_i))^r \qquad \text{for all } i$$

then $d(\chi) \in \widehat{D^1}$ and

$$C' = < d(\chi) > \quad ; \quad d(\chi)^3 = 1$$

is in fact a complement for D^1. Now

$$\chi(\varphi(\alpha_i)) = (\chi(\alpha_i))^2 \quad \text{for all } i \; .$$

But $r \equiv 2 \pmod 3$ and

$$\chi(\alpha_i) = 1 \quad \text{or} \quad a^{(r^2 - 1)/3} \quad \text{or} \quad a^{2(r^2 - 1)/3} \; .$$

Hence

$$\chi(\varphi(\alpha_i)) = (\chi(\alpha_i))^2 = (\chi(\alpha_i))^r$$

i.e. $d(\chi) \in \widehat{D^1}$, and our result is proved.

§ (III) <u>The Groups of the Type A_ℓ^1</u> .

Here

(7.4) $$\hat{D}^1/D^1 \cong \hat{h}^1/h^1 \cong \hat{H}^1/H^1 \quad ;$$

$$\left|\frac{\hat{H}^1}{H^1}\right| = d = \text{g.c.d.}\ (\ell+1,\ q+1)$$

where

$$|K| = p^{2n} = r^2 \quad .$$

We prove the following

<u>Lemma 7.5</u>

Suppose $d = \text{g.c.d.}\ (\ell+1,\ r+1)$ is odd and $r+1 = d.u.$ where g.c.d. $(d,\ u) = 1$.

Then there is a complement C' for D^1 in $\hat{D}^1$.

<u>Proof</u>

Now $r+1 = d.u$;

$$\therefore \quad r-1 = du - 2 \ .$$

$$\therefore \quad r^2-1 = (r+1)(r-1) = du(du-2)$$

and $\dfrac{r^2-1}{d} = u\,(du-2)$. As $(u,d) = 1$ and d is odd, d and $u\,(du-2)$ are coprime. Let us now define a character χ of P_r such that

$$\chi(\alpha_1) = a^{(r^2-1)/d} \quad ; \quad \chi(\alpha_\ell) = a^{(d-1)(r^2-1)/d}$$

$$\text{and} \quad \chi(\alpha_i) = 1 \quad \text{for all} \quad i \neq 1\ ,\ \ell\ .$$

Following an exactly similar argument as used in (lemma 7.6; (1)) we see that χ^i , where χ is defined as above, cannot be extended to a character

of P . Hence if we can show that $\chi(\varphi(\alpha_i)) = \chi(\alpha_i)^r$ for all i then

$$C' = \langle d(\chi) \rangle \ ; \qquad d(\chi)^d = 1$$

forms a complement for D^1 in $\widehat{D}^1$.

But modulo r^2-1 we have

$$(d-1)\left(\frac{r^2-1}{d}\right) \equiv q\left(\frac{r^2-1}{d}\right) ,$$

since

$$(r+1-d)\left(\frac{r^2-1}{d}\right) = (d.u-d)\left(\frac{r^2-1}{d}\right)$$

$$\equiv (u-1)(r^2-1)$$

$$\equiv 0 \pmod{r^2-1} .$$

Hence

$$\chi(\varphi(\alpha_1)) = \chi(\alpha_1)^r .$$

Similarly

$$q(d-1)\left(\frac{r^2-1}{d}\right) \equiv \frac{r^2-1}{d} \quad \text{gives}$$

$$\chi(\varphi(\alpha_\ell)) = (\chi(\alpha_\ell))^r .$$

Since

$$\chi(\alpha_i) = 1 \qquad i \neq 1, \ \ell$$

we have

$$\chi(\varphi(\alpha_i)) = \chi(\alpha_i)^r \ \text{ for all } \ i .$$

CHAPTER 8

THE GROUPS OF SUZUKI AND REE

§ (I) Suzuki Groups.

We shall first give the Lie theoretical interpretation of Suzuki groups (cf. [14]). Let G be a Chevalley group of type B_2 over a field K of characteristic 2. We also assume that K admits an automorphism $t \to t^\theta$ such that $\theta^2 = 1$. If α and β are the fundamental roots of the corresponding Lie algebra such that $2\alpha + \beta$ is a root then it turns out that G admits an automorphism σ which is given by

$$x_{\pm\alpha}(t) \longleftrightarrow x_{\pm\beta}(t^\theta) \quad ,$$

$$x_{\pm(2\alpha+\beta)}(t) \longleftrightarrow x_{\pm(\alpha+\beta)}(t^\theta) \quad .$$

If U (resp. V) denote the subgroup of G generated by all $x_r(t)$ with $r > 0$ (resp. $r < 0$), let U^1 (resp. V^1) denote the group of elements in U (resp. in V) left invariant by σ. The group G^1 generated by U^1 and V^1 turns out to be simple when K has more than 2 elements and is a Suzuki group when K is finite.

An automorphism δ of G^1 is shown ([2], [20]) to be a product $x.f$ of an inner automorphism x and a field automorphism f. Suzuki (p. 140, [20]) also proves that no field automorphism can be an inner automorphism.

Hence we have

Lemma (8.1)

The group of field automorphisms forms a complement for $\mathrm{Inn}\,(G^1)$ in $\mathrm{Au}\,(G^1)$.

§ (II) Ree Groups.

Following the method which emerges naturally when Suzuki's method is considered from a Lie theoretical point of view. Ree constructed two families of simple groups which were previously unknown.

First, let G be a Chevalley group of the type G_2 and suppose the complete system of 12 distinct roots is given as

$$\{ \pm r_i \, , \, r_i - r_j \;\mid\; i \, , \, j = 1, 2, 3 \;\; ; \;\; i \neq j \}$$

where $r_1 + r_2 + r_3$ is not a root.

Define a function λ on the root system as

$$\lambda(\pm r_i) = 1 \quad , \quad \lambda(r_i - r_j) = 3 \, .$$

If P_r denotes the group (additive) generated by the root system define a homomorphism Ψ of P_r by

$$\Psi(r_1) = r_2 - r_3 \quad , \quad \Psi(r_2) = r_1 - r_2 \quad .$$

Then there is a permutation $r \rightarrow \bar{r}$ of the root system, which is of order two such that

$$\bar{r} \quad \lambda(r) = \Psi(r)$$

$$(\overline{-r}) = -\bar{r} \qquad \text{and}$$

$$\lambda(r)\,\lambda(\bar{r}) = 3 .$$

Finally we suppose K to be a perfect field of characteristic 3 and such that K admits an automorphism θ satisfying

$$3\theta^2 = 1 .$$

Then the group G admits an automorphism σ such that

$$x_r(t) \to x_{\bar{r}}\left(t^{\lambda(\bar{r})\theta}\right) .$$

Let U^1 (resp. V^1) be the group of elements of U (resp. of V) which are invariant under σ. The group G^1 generated by U^1 and V^1 has been shown to be simple by Ree ([14]) provided K has more than 3 elements.

Another family of simple groups are obtained from the Chevalley groups G of the type F_4.

Let $\{ r_i , r_i + r_j , \frac{1}{2}(r_i + r_j + r_k + r_\ell) \}$

where $i, j, K, \ell = \pm 1, \pm 2, \pm 3, \pm 4$; $|i|$, $|j|$, $|K|$, $|\ell|$ are distinct ; $r_{-i} = -r_i$ for all i.

Let $(r_i \mid r_j) = 1$ if $i = j$

$= 0$ if $i = j$.

Extend this mapping for the whole root system and let

$$\lambda(r) = (r|r) , \quad r = a \text{ root} .$$

Define a mapping Ψ by

$$\Psi(r_1) = r_1 + r_2 , \quad \Psi(r_2) = r_1 - r_2$$

$$\Psi(r_3) = r_3 + r_4 , \quad \Psi(r_4) = r_3 - r_4 .$$

Extend Ψ for the root system.

Then there is a permutation $r \to \bar{r}$ of order 2 of the root system such that

$$\Psi(r) = \lambda(r)\, \bar{r}$$

$$(\overline{-r}) = -\bar{r}$$

$$\lambda(r)\, \lambda(\bar{r}) = 2 \quad \text{for any root } r .$$

If K denotes the base field then suppose K has characteristic 2. Let θ be an automorphism of K such that

$$2\theta^2 = 1 .$$

Then the group G admits an automorphism σ such that

$$x_r(t)^\sigma = x_{\bar{r}}(t^{\lambda(\bar{r})\theta}) .$$

If U^1 (resply. V^1) denotes the elements in U (resp. V), invariant under σ, let G^1 be the group generated by U^1 and V^1. Ree ([13]) has shown that the group G^1 is always simple provided K has more than 2 elements.

§ (III) Automorphisms of Ree Groups.

If the base field K is finite, every field automorphism commutes with the special field automorphism θ taken for the construction of the Ree groups. Hence every automorphism $t \to t'$ of the field K induces an automorphism $x_r(t) \to x_r(t')$ of G^1. These are called field automorphisms of G^1.

The following result is due to Ree ([13] , [14])

(8.2) Let G^1 be a Ree group. Suppose K has more than 3 elements when G^1 is of type (G_2) and K has more than 2 elements when G^1 is of the type (F_4). Then each automorphism ρ of G^1 is uniquely expressed as the product $x.f$ of an inner automorphism x and a field automorphism f.

We immediately get

Lemma (8.3)

If G^1 is a simple finite Ree group then $\mathrm{Inn}(G^1)$ has a complement in $\mathrm{Au}(G)$.

Proof

Since the presentation $x\,f$ for the automorphism ρ is unique the lemma is trivial.

BIBLIOGRAPHY

1. R. Bercov, On groups without abelian composition factors. J. of Algebra, Vol. 5, No. 1 (1967). pp. 106 - 109.

2. R. W. Carter, Simple groups and simple Lie algebras. J. London Math. Soc. 40 (1965). pp. 193 - 240.

3. C. Chevalley, Sur Certains Groups simples. Tohoku Math. J. 7 (1965). pp. 14 - 66.

4. L. e. Dickson, Theory of Linear groups in an arbitrary field. Trans. Amer. Math. Soc. 2 (1901). pp. 363 - 394.

5. L. E. Dickson, A new system of simple groups. Math. Annales. 60 (1905). pp. 137 - 150.

6. N. Jacobson, Lie algebras. Interscience track No. 10 (New York 1962).

7. M. Hall, The Theory of groups. McMillan Comp. (New York 1959).

8. Harish-Chandra, On some applications of the Universal enveloping algebra of a semi-simple Lie algebra. Trans. of Amer. Math. Soc. 70 (1951), pp. 28 - 96.

9. D. W. Miller, On a theorem of Holder, Amer. Math. Month. 65 (1958). pp. 252 - 254.

10. B. H. Neumann, Twisted Wreath product of groups. Archiv der Math. 14 (1963). pp. 1 - 6.

11. B. H. Neumann, On a theorem of Auslander and Lyndon. Archiv der Math. 13 (1962). pp. 4 - 9.

12. R. Ree, On some simple groups defined by Chevalley Trans. Amer. Math. Soc. 84 (1957). pp. 312 - 400.

13. R. Ree, A family of simple groups associated with the simple Lie algebra of type (F_4). Amer. J. Math. 83 (1961). pp. 401 - 420.

14. R. Ree, A family of simple groups associated with the simple Lie algebra of type (G_2). Amer. J. Math. 83 (1961). pp. 432 - 462.

15. W. R. Scott, Group Theory. Prentice Hall, 1964.

16. R. Steinberg, Automorphisms of finite Linear groups. Can. J. Math. 12 (1960). pp. 606 - 615.

17. R. Steinberg, Generators for simple groups. Can. J. Math. 14 (1962). pp. 277 - 283.

18. R. Steinberg, Variations on a theme of Chevalley. Pac. J. Math. 9 (1959). pp. 875 - 891.

19. M. Suzuki, A new type of simple groups of finite order. Proc. Nat. Acad. Sci. U.S.A. 46 (1960) pp. 868 - 870.

20. M. Suzuki, On a class of doubly transitive groups. Annals of Math. (2), 75 (1962). pp. 105 - 145.